https://lajc.epn.edu.ec

ESCUELA POLITÉCNICA NACIONAL

VOLUME 7, ISSUE 2
DECEMBER 2020
ISSN: 1390-9266

EDITOR IN CHIEF
PhD. Marco Santórum G.
Escuela Politécnica Nacional,
Ecuador.

LATIN-AMERICAN JOURNAL OF COMPUTING

IAIC

Vol VII, Issue 2, December 2020

ESCUELA POLITÉCNICA NACIONAL

EPN

https://www.epn.edu.ec

ISSN: 1390 -9266 – 2020 LAJC

MISIÓN

La Escuela Politécnica Nacional es una Universidad pública, laica y democrática que garantiza la libertad de pensamiento de todos sus integrantes, quienes están comprometidos con aportar de manera significativa al progreso del Ecuador. Formamos investigadores y profesionales en ingeniería, ciencias, ciencias administrativas y tecnología, capaces de contribuir al bienestar de la sociedad a través de la difusión del conocimiento científico que generamos en nuestros programas de grado, posgrado y proyectos de investigación. Contamos con una planta docente calificada, estudiantes capaces y personal de apoyo necesario para responder a las demandas de la sociedad ecuatoriana.

VISIÓN

En el 2024, la Escuela Politécnica Nacional es una de las mejores universidades de Latinoamérica con proyección internacional, reconocida como un actor activo y estratégico en el progreso del Ecuador. Forma profesionales emprendedores en carreras y programas académicos de calidad, capaces de aportar al desarrollo del país, así como promover y adaptarse al cambio y al desarrollo tecnológico global. Posiciona en la comunidad científica internacional a sus grupos de investigación y provee soluciones tecnológicas oportunas e innovadoras a los problemas de la sociedad.

La comunidad politécnica se destaca por su cultura de excelencia y dinamismo al servicio del país dentro de un ambiente de trabajo seguro, creativo y productivo, con infraestructura de primer orden.

ACCIÓN AFIRMATIVA

La Escuela Politécnica Nacional es una institución laica y democrática, que garantizar la libertad de pensamiento, expresión y culto de todos sus integrantes, sin discriminación alguna. Garantiza y promueve el reconocimiento y respeto de la autonomía universitaria, a través de la vigencia efectiva de la libertad de cátedra y de investigación y del régimen de cogobierno.

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

https://fis.epn.edu.ec

ISSN: 1390 -9266 – 2020 LAJC

MISIÓN

La Facultad de Ingeniería de Sistemas es el referente de la Escuela Politécnica Nacional en el campo de conocimiento y aplicación de las Tecnologías de Información y Comunicaciones; actualiza en forma continua y pertinente la oferta académica en los niveles de pregrado y postgrado para lograr una formación de calidad, ética y solidaria; desarrolla proyectos de investigación, vinculación y proyección social en su área científica y tecnológica para solucionar problemas de transcendencia para la sociedad.

VISIÓN

La Facultad de Ingeniería de Sistemas está presente en posiciones relevantes de acreditación a nivel nacional e internacional y es referente de la Escuela Politécnica Nacional en el campo de las Tecnologías de la Información y Comunicaciones por su aporte de excelencia en las carreras de pregrado y postgrado que auspicia, la calidad y cantidad de proyectos de investigación, vinculación y proyección social que desarrolla y su aporte en la solución de problemas nacionales a través del uso intensivo y extensivo de la ciencia y la tecnología.

CEDIA

CORPORACIÓN ECUATORIANA
PARA EL DESARROLLO DE LA
INVESTIGACIÓN Y LA ACADEMIA

Gonzalo Cordero 2-122 y J. Fajardo Esq.
Teléfono (+593) 7 407 9300
info@cedia.org.ec • Cuenca - Ecuador

www.cedia.edu.ec

ISSN: 1390 -9266 – 2020 LAJC

Promovemos la investigación y desarrollo de proyectos innovadores que vinculan a las instituciones mediante concursos e iniciativas. Impulsamos y facilitamos recursos a estudiantes, docentes, profesionales e investigadores con la impresión de esta recopilación científica.

Designed and Printed by
CEDIA

LATIN-AMERICAN JOURNAL OF COMPUTING

Vol VII, Issue 2, December 2020

ISSN: 1390-9266

Published by:
Escuela Politécnica Nacional
Facultad de Ingeniería de Sistemas

Quito – Ecuador

LATIN-AMERICAN JOURNAL OF COMPUTING

Mailing Address

Escuela Politécnica Nacional,
Facultad de Ingeniería de Sistemas
Ladrón de Guevara E11-253, La Floresta
Quito-Ecuador, Apartado Postal: 17-01-2759

Web Address

https://lajc.epn.edu.ec/

E-mail

lajc@epn.edu.ec

Frequency

2 issues per year

ISSN: 1390 -9266 – 2020 LAJC

Published by

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistemas
Ecuador

Editor in Chief

Marco Santórum G. PhD.
Escuela Politécnica Nacional, Ecuador

Editorial Committee

José Aguilar PhD.
Universidad de los Andes, Venezuela
aguilar@ula.ve
Matthew Bradbury PhD.
University of Warwick, UK
m.bradbury@warwick.ac.uk
Lucía Carrión PhD.
University of Technology Sydney, Australia
lucia.c.carrion@alumni.uts.edu.au
Hagen Lauer PhD.
Fraunhofer SIT, Germany
hagen.lauer@sit.fraunhofer.de
Diana Ramírez PhD (c).
Universidad Pompeu Fabra, España
diana.ramirez@upf.edu
Marco Santórum G. PhD.
Escuela Politécnica Nacional, Ecuador
marco.santorum@epn.edu.ec

Associate Editors

Sandra Sánchez Gordón, PhD.
Escuela Politécnica Nacional, Ecuador
sandra.sanchez@epn.edu.ec
Robert Enríquez, PhD.
Universidad Central del Ecuador, Ecuador
renriquez@uce.edu.ec
Luis Tello Oquendo, PhD.
Universidad Nacional de Chimborazo, Ecuador
lptelloq@ieee.org

Assistant Editors

Lic. Dayana Marcillo
Escuela Politécnica Nacional, Ecuador
dayana.marcillo@epn.edu.ec

Jorge Miño
Escuela Politécnica Nacional, Ecuador
jorge.mino@epn.edu.ec

EDITORIAL

Sandra Sánchez Gordón, PhD.

Associate Editor
Escuela Politécnica Nacional, Ecuador

Estimados lectores,

Bienvenidos al Número 2 Volumen 7 de Latin-American Journal of Computing. Este es el segundo número que ponemos a disposición durante la pandemia global de COVID-19 y con él se cierra la actividad del 2020. En esta oportunidad, los editores de LAJC deseamos agradecer las muchas horas de dedicación en el cumplimiento de su labor profesional, académica e investigativa de nuestros lectores y colaboradores durante esta época.

En este número regular, me complace presentar una interesante variedad de artículos de investigación relevantes en sus respectivos campos. Esperamos que los ocho temas seleccionados logren interesar e incentivar a nuestros lectores en sus diversas actividades. Una breve sinopsis de cada uno se muestra a continuación.

El artículo “Agricultura digital en el cultivo de pitahaya” presenta una solución tecnológica que provee información relevante para una agricultura de precisión. Dicha solución se implantó en el cantón Palora, Provincia Morona Santiago, Ecuador donde existen 1528 hectáreas de sembríos de pitahaya. En el artículo “Detección de anomalías bajo un modelo de seguridad cognitiva” se implementa una arquitectura para diferenciar el comportamiento del tráfico de red benigno del malicioso, como apoyo a los procesos cognitivos de los analistas de seguridad. En el tercer artículo “Diseño e implementación de una red inalámbrica de sensores con tecnología LoRa para monitoreo industrial” se propone una arquitectura para comunicaciones de corto alcance con equipos de bajo costo que ha sido validada en dos escenarios industriales. En el estudio realizado en “Evaluación comparativa del rendimiento de controladores SDN de código abierto” se crea una red definida por software utilizando mecanismos de virtualización livianos para comparar latencia, desempeño y escalabilidad de tres controladores de protocolo abierto. Los autores de “Implementación de un virus enfocado en dispositivos móviles Android. Un evento de hacking ético” utilizan una plataforma virtualizada para realizar pruebas de penetración a sistemas Androide para estudiar las vulnerabilidades de dichos sistemas. El artículo “Procesamiento digital de imágenes en la creación de prototipo de sistema inteligente para detección y reconocimiento de texto en etiquetas de conductores eléctricos recubiertos” se emplea una base de datos de imágenes de cables de diverso color, color del texto, tipo de cable y calibre, similares a los que se usan en plantas industriales, obteniendo tasas de error promedio de 6.54%, 3.97% y 2.53%. El siguiente artículo “Registrador de datos pluviométricos basado en el microcontrolador ATMEL y el transceptor LoRa” se implementa una estación meteorológica de bajo consumo de energía y costos reducidos para la adquisición, almacenamiento y transmisión de datos. Durante el confinamiento, los autores del artículo “Uso de la tecnología en Industria 4.0 para apoyar en el combate de la epidemia por COVID-19 a través de un dispensador para higiene de las manos usando dispositivos de construcción local” usaron materiales de fácil adquisición y bajo costo para fabricar un dispositivo que detecta la presencia de las manos del usuario frente al ducto del dispensador de líquido sanitizante.

Agradezco a los autores y revisores de este número por su valiosa y generosa contribución. Para finalizar, un merecido reconocimiento anual a todos los autores y revisores que han apoyado desinteresadamente a la revista LAJC desde sus inicios en el 2014.

¡Disfruten la lectura de este número!

ISSN: 1390 -9266 – 2020 LAJC

Dear readers,

Welcome to Number 2 Volume 7 of Latin-American Computing Journal. This is the second issue that we make available during the global COVID-19 pandemic and with it the 2020 activity closes. On this occasion, the editors of LAJC wish to thank the many hours of dedication in the fulfillment of their professional, academic and research responsibilities of our readers and collaborators during this time.

In this regular issue, I am pleased to present an interesting variety of relevant research articles in their respective fields. We hope that the eight selected topics will generate interest and encourage our readers in their various activities. A brief synopsis of each is shown below.

The article "Digital agriculture in pitahaya crop" presents a technological solution that provides relevant information for precision agriculture. This solution was implemented in the Palora region, Morona Santiago Province, Ecuador where there are 1,528 hectares of pitahaya crops. In the article "Anomaly detection under a cognitive security model", an architecture is implemented to differentiate the behavior of benign from malicious network traffic, to support the cognitive processes of security analysts. In the third article "Design and implementation of a wireless sensor network with LoRa technology for industrial monitoring", an architecture for short-range communications with low-cost equipment is proposed. This solution was validated in two industrial scenarios. The study “A comparative evaluation of the performance of open-source SDN controllers" creates a software-defined network using lightweight virtualization mechanisms to compare latency, performance, and scalability of three open protocol controllers. The authors of “An implementation of a virus focused on mobile devices with Android. An Ethical Hacking Event” use a virtualized platform to perform penetration tests on Android systems to study the vulnerabilities of said systems. The article "Digital image processing in the creation of an intelligent system prototype for text detection and recognition in the labeling process of electrical cable" uses a database of images of cables of different color, text color, cable type and caliber, similar to those used in industrial plants, obtaining average error rates of 6.54%, 3.97% and 2.53%. The following article “Rain gauge data logger based on ATMEL microcontroller and LoRa transceiver” implements a weather station with low power consumption and reduced costs for data acquisition, storage, and transmission. During the confinement, the authors of the article "Use of technology in Industry 4.0 to support the fight against the COVID-19 epidemic through a hand hygiene dispenser using locally built devices" used easily available and low cost materials to manufacture a device that detects the presence of the user's hands in front of the sanitizing liquid dispenser duct.

I thank the authors and reviewers of this issue for their valuable and generous contribution. Finally, a well-deserved annual recognition to all the authors and reviewers who have selflessly supported LAJC since its inception in 2014.

Enjoy reading this issue!

LATIN-AMERICAN JOURNAL OF COMPUTING

We are most grateful to the following individuals for their time and commitment to review manuscripts for Latin American Journal of Computing – LAJC

ISSN: 1390 -9266 – 2020 LAJC

Reviewers

Patricia Acosta, PhD.
Universidad de Las Américas
Josafa Aguiar, PhD.
Escuela Politécnica Nacional
Roberto Andrade, MSc.
Escuela Politécnica Nacional
Boris Astudillo, MSc.
Escuela Politécnica Nacional
Fabián Astudillo, PhD.
Universidad de Cuenca
Lorena Barona, PhD.
Escuela Politécnica Nacional
Jhonattan Barriga, MSc.
Escuela Politécnica Nacional
Eduardo Benavides, MSc.
Escuela Politécnica Nacional
Nancy Betancourt, MSc.
Escuela Politécnica Nacional
Susana Cadena, PhD.
Universidad Central del Ecuador
Iván Carrera, MSc.
Escuela Politécnica Nacional
Juan Pablo Carvallo, PhD.
Universidad del Azuay
Juan Córdova, MSc.
Universidad del Azuay
Heitor Costa, PhD.
Federal University of Lavras
Pablo del Hierro, PhD.
Escuela Politécnica Nacional
Robert Enríquez, PhD.
Universidad Central del Ecuador
Vera Ferreira, PhD.
Federal University of the Pampa
Denys Flores, PhD.
Escuela Politécnica Nacional, Ecuador
Miguel Flores, PhD.
Escuela Politécnica Nacional
Walter Fuertes, PhD.
Universidad de las Fuerzas Armadas
Julián Galindo, PhD.
Escuela Politécnica Nacional
José García Rodríguez, PhD.
Universidad de Alicante
Fredy Gavilanes, MSc.
Escuela Politécnica Nacional
Maria Hallo, PhD.
Escuela Politécnica Nacional
Myriam Hernández, PhD.
Escuela Politécnica Nacional
Cindy López, MSc.
Escuela Politécnica Nacional
Gabriel López, MSc.
Escuela Politécnica Nacional
Edison Loza, PhD.
Escuela Politécnica Nacional
Sergio Luján Mora, PhD.
Universidad de Alicante
Marco Molina, PhD.
Escuela Politécnica Nacional
Marcela Mosquera, MSc.
Escuela Politécnica Nacional
Rosa Navarrete, PhD.
Escuela Politécnica Nacional
Freddy Tapia, MSc.
Escuela Politécnica Nacional
Luis Tello Oquendo, PhD.
Universidad Nacional de Chimborazo
Edgar Torres, MSc.
Escuela Politécnica Nacional
Jenny Torres, PhD.
Escuela Politécnica Nacional
Henry Paz, MSc.
Escuela Politécnica Nacional
Rodrigo Padilla, MSc.
Universidad de Cuenca
Diego Pinto, MSc.
Universidad de las Fuerzas Armadas ESPE
Lorena Recalde, PhD.
Escuela Politécnica Nacional
Henry Roa, PhD.
Pontificia Universidad Católica del Ecuador
Daniel Sanaguano, MSc.
Escuela Politécnica Nacional
Franklin Sánchez, MSc.
Escuela Politécnica Nacional
Manuel Sánchez Rubio. PhD.
Universidad Internacional de la Rioja
Sandra Sánchez Gordón, PhD.
Escuela Politécnica Nacional
Luis Urquiza, PhD.
Escuela Politécnica Nacional
Ángel Valdivieso, PhD.
Escuela Politécnica Nacional
Víctor Velepucha, MSc.
Escuela Politécnica Nacional
Diana Yacchirema, PhD.
Escuela Politécnica Nacional
Yasmina Vizuete, MSc.
Escuela Politécnica Nacional

TABLE OF CONTENTS

Agricultura digital en el cultivo de Pitahaya
Digital agriculture in Pitahaya crop
Ángel Llerena Zambrano — 22

Detección de Anomalías Bajo un Modelo de Seguridad Cognitiva
Anomaly Detection Under a Cognitive Security Model
Jonathan Herrera
Roberto Omar Andrade
Miguel Flores
Susana Cadena — 34

Diseño e implementación de una red inalámbrica de sensores con tecnología LoRa para monitoreo industrial
Design and implementation of a wireless sensor network with LoRa technology for industrial monitoring
Adrián E. Heredia
Paúl F. Lucero
Fabián Astudillo Salinas
Andrés Vázquez Rodas — 48

Evaluación comparativa del rendimiento de controladores SDN de código abierto
A comparative evaluation of the performance of open-source SDN controllers
Daniel Haro Mendoza
Luis Tello Oquendo
Luis A. Marrone — 64

Implementación de un virus enfocado en dispositivos móviles Android. Un evento de hacking ético
An implementation of a Virus Focuses on Mobile Devices with Android. An Ethical Hacking Event
Carlos Andrés Estrada Vásquez
Walter Fuertes
Amy Rashell Sánchez Cárdenas — 78

Procesamiento digital de imágenes en la creación de prototipo de sistema inteligente para detección y reconocimiento de texto en etiquetas de conductores eléctricos recubiertos
Digital image processing in the creation of an intelligent system prototype for text detection and recognition in the labeling process of electrical cable
Juan J. Navarro
Carolina Reta — 92

Registrador de datos pluviométricos basado en el microcontrolador ATMEL y el transceptor LoRa
Rain gauge data logger based on ATMEL microcontroller and LoRa transceiver
Kevin Piedra Orellana
Fabián Astudillo Salinas
Geovany Lupercio Novillo
Andrés Vázquez Rodas
Ismael Minchala Ávila — 108

Uso de la Tecnología en Industria 4.0 para apoyar en el combate de la epidemia por COVID-19 a través de un dispensador para higiene de las manos usando dispositivos de construcción local
Use of Technology in Industry 4.0 to support the fight against the COVID-19 epidemic through a hand hygiene dispenser using locally built devices
Andrés Ganán
Cristian Ganán
Robert Enríquez — 124

ISSN: 1390 -9266 – 2020 LAJC

LATIN-AMERICAN JOURNAL OF COMPUTING (LAJC). Vol VII, Issue 2, December 2020

Agricultura digital en el cultivo de Pitahaya

Digital agriculture in Pitahaya crop

ARTICLE HISTORY

Received 30 September 2020
Accepted 16 October 2020

Ángel Llerena Zambrano
Departamento IoT
Telcombas S.A.
Guayaquil, Ecuador
af.llerena@telcombas.com

Agricultura digital en el cultivo de Pitahaya

Digital agriculture in Pitahaya crop

Ángel Llerena Zambrano
Departamento IoT
Telcombas S.A.
Guayaquil, Ecuador
af.llerena@telcombas.com

Abstract — Digital agriculture has arrived to solve the production problem that exists in the land, the optimization of agricultural processes through sensors with IoT technology are being a great help so that farmers can produce more on their land and use the available resources of a more effective way. The trial that was carried out in the Palora sector in the cultivation of pitahaya, testing this new technology, resulted in having the data in real time allowing better decisions to be made when carrying out agricultural work without the need to be present in the plantation, such as Consequently, the environmental impact is minimized and a greater profitability of the crop is obtained. Once the information analysis had been carried out, it was determined that the area where the pitahaya crop is located does meet the necessary characteristics for the development of the crop, this could be contrasted by analyzing the data and monitoring the parameters in the intuitive agriculture module platform. The results obtained are an average of 7 mm / day of water in the pluviosity parameter, in terms of solar radiation, measurements were obtained with a ceiling of 2581.51 PAR, on the other hand, soil moisture had peaks of up to 16.40 cb, finally the temperature reached levels of 35.09 ° c.

Keywords — Digital agriculture, precision agriculture, sensors, artificial intelligence

Resumen — La agricultura digital ha llegado para solventar la problemática de producción que existe en los terrenos, la optimización de los procesos agrícolas mediante sensores con tecnología IoT están siendo una gran ayuda para que los agricultores puedan producir más en sus terrenos y utilizar los recursos disponibles de una manera más eficaz. En el ensayo que se realizó en el sector de Palora en el cultivo de pitahaya, se probó esta nueva tecnología, obteniendo como resultado de las pruebas realizadas la generación de datos en tiempo real que permiten tomar mejores decisiones al momento de realizar las labores agrícolas sin necesidad de estar presentes en la plantación, como consecuencia se minimiza el impacto ambiental y se obtiene una mayor rentabilidad del cultivo. Una vez realizado el análisis de la información, se determinó que la zona donde está ubicado el cultivo de pitahaya si cumple con las características necesarias para el desarrollo del cultivo, esto se pudo contrastar mediante la analítica de los datos y el seguimiento de los parámetros en la plataforma intuitiva modulo agricultura. Los resultados obtenidos son de un promedio de 7 mm/día de agua en el parámetro de pluviosidad, en cuanto a la radiación solar se obtuvo mediciones con un tope de 2581.51 PAR, por otro lado, la humedad del suelo tuvo picos de hasta 16.40 cb, finalmente la temperatura llego hasta niveles de 35.09 °c.

Palabras clave — *Agricultura digital, agricultura de precisión, sensores, inteligencia artificial*

ISSN: 1390 -9266 – 2020 LAJC

I. INTRODUCCIÓN

La agricultura moderna está basada en principios muy básicos tales como la eficiencia, reducción y conservación de los recursos no renovables que son indispensables para la producción de cultivos.

Es importante conocer con exactitud las características biológicas y agronomías del cultivo de pitahaya, implementando agricultura de precisión en los terrenos de producción. Los sensores que pueden medir estos parámetros son los medidores de temperatura, pluviosidad, luminosidad, humedad relativa, humedad de suelo entre otros parámetros, permitiendo tener un mayor control de la producción, optimizando el uso y aplicación de productos fitosanitarios.

En la actualidad se están desarrollando una gran variedad de softwares para los diferentes cultivos incorporando las necesidades nutricionales, climáticas y edáficas para ayudar a los agricultores a minimizar los costos de producción por la aplicación innecesaria de muchos insumos agrícolas en sus plantaciones logrando así ser más competitivos. El manejo e interpretación de la data es una herramienta que se utiliza para proyectar o simular con una gran precisión eventos que se puedan suscitar y el agricultor pueda estar mejor preparado.

El uso de esta tecnología se la utilizó en este proyecto para poder optimizar los procesos agrícolas semanales que se presentan en el cultivo, de esta manera ahorra costos de producción, que generan mayor rentabilidad al productor al momento de la cosecha y comercialización de su cultivo. Adicional, con la tecnología IoT el productor tiene una herramienta que le facilitará la toma decisiones en tiempo real, cuando no esté presente sobre el cultivo, y dar indicaciones a sus trabajadores si es necesario aplicar un insumo agrícola, suministrar riego o parar de regar.

La implementación de esta estación de sensores se la realizó en el cultivo de pitahaya, la conectividad para la trasmisión de los datos se consideró un chip celular 3G, para enviar los datos recolectados por los sensores hacia la nube y finalmente poder ver los datos en la plataforma desarrollada modulo agricultura.

II. CULTIVO DE PITAHAYA

A. Pitahaya a nivel mundial y en el Ecuador

La pitahaya o también conocida como fruta dragón pertenece según su clasificación taxonómica a la familia Cactaceae, género Hylocereus, especie H. undatus, H. mengalanthus [1].

Es conocida a nivel mundial con más de 2000 especies, localizadas en el continente asiático y americano específicamente en los países como México, Nicaragua, Guatemala, Costa Rica, Ecuador y Colombia [2].

En el Ecuador el cantón de Palora, Provincia Morona Santiago perteneciente a la región de la Amazonia es uno de los mayores productores Pitahaya, en esta zona existen 672 productores de pitahaya que tienen sembradas 1528 hectáreas, de las que actualmente 664 están en producción, indican datos del Ministerio de Agricultura y ganadería (MAG) [4].

El cantón Palora posee un clima tropical húmedo, temperatura promedio de 22.5ºC, precipitación anual 3000 - 4000 mm, precipitaciones altas abarcan desde mes de julio a mes de diciembre y llegan hasta 5.000mm; y el verano con las precipitaciones bajas hasta 200 mm se ubica en los meses de enero, febrero y marzo y con una humedad relativa del 85% [3].

Su comercialización corresponde a dos variedades la roja y la amarilla. La variedad roja tiene su corteza de color roja no posee espinas, su pulpa es de color blanca con tonalidades rojizas y pequeñas semillas de color negro, la diferencia con la variedad amarilla es el color de su cascara, si posee espinas y su sabor es más dulce que la otra variedad como se observa en las figura 1 [5][8][9].

Fig. 1. Fruto de pitahaya roja [8].

Fig. 2. Fruto de pitahaya amarilla [9].

B. Generalidades del cultivo

Pitahaya es un cultivo perenne terrestre rastrero con abundantes ramas, puede alcanzar hasta dos metros de largo, posee 2 raíces una primaria cuya función es de absorción y las demás raíces secundarias ayudan a sostener la planta, su tallo son vainas muy ramificadas de color verde en donde se encuentran espinas o también llamadas hojas modificadas en donde nacen las flores hermafroditas con una combinación de colores blancos amarillos o rasados, tiene ciclos de floración de 5 o 6 ciclos y pueden necesitar de polinización cruzada, el fruto es de forma globosa y tiene de 8 a 15 cm de largo por 6 a 10 cm de diámetro con cascaras de color rojo o amarillo como se observa en las figuras 1 y 2 [6].

C. Requerimientos edafoclimáticos

Los requerimientos edafológicos necesarios para la correcta producción del cultivo de pitahaya son diversos entre ellos está el clima la pitahaya es un cultivo de climas cálidos subhúmedos con un rango de temperatura ideal de 16°C hasta 25°C, aunque también se puede dar en climas secos y tolerar una temperatura de hasta 38°C, tiene un requerimiento de lluvias moderadas, precipitación óptima oscila entre 500 a 700mm anuales. La luminosidad es vital para sus procesos fisiológicos en especial para iniciar la floración, el porcentaje de luminosidad es de 70% exposición solar y un 30% en sombra [7].

Otro aspecto necesario es el sustrato, la pitahaya es una planta adaptable a cualquier tipo de sustrato, pero se desarrolla mejor en suelos franco-arenosos y húmedos con un pH ligeramente ácido entre 5,5 a 6,5. Con una humedad del suelo 50% de humedad y una humedad relativa del 80 a 85% [7].

III. AGRICULTURA DIGITAL

La agricultura digital nos permite utilizar un sin número de herramientas tecnológicas que se pone a disposición para el mundo del agro, la cual consiste en monitorear diferentes variables del suelo, ambiente, recolectando y analizando los datos.

Es una solución tecnológica que permite por medio de diferentes sensores recopilar información de los factores que afectan a una plantación y enviar los datos a una plataforma intuitiva online para una correcta interpretación y toma de decisiones por parte de los agricultores.

La implementación de esta solución brinda al agricultor una ayuda y acompañamiento en los procesos durante todo el ciclo productivo del cultivo.

Sabemos que el mundo ha venido evolucionando y la agricultura no se podía quedar atrás, siendo uno de los pilares mas importantes en el desarrollo del ser humano. Por lo tanto, la transformación de la agricultura convencional a agricultura digital es una realidad. Es importante conocer cuántos milímetros de agua tiene un terreno, la velocidad del viento es facto predisponente para la aplicación de un producto foliar, conocer cuando el suelo requiere de agua, o cuando el cultivo esta expuesto a mucha radiación solar. Son factores que ayudan a una correcta toma de decisión para poder actuar ante estas variables que se presentan a diario en las explotaciones agrícolas. Sin duda alguna es una solución que en todo momento permitirá al agricultor tomar mejores decisiones en su día a día.

La tecnología en la agricultura aumenta un mayor rendimiento de los cultivos, mejor la calidad, ayuda a comprender qué factores gobiernan el crecimiento y el rendimiento de los cultivos y garantizar la seguridad alimentaria. Así como también reduce intervenciones humanas bajando el rubro del personal, disminución de la utilización innecesaria de fertilizantes, pesticidas y combustible, reduce las probabilidades de enfermedades o condiciones climáticas adversas luchando contra las sequías, la escasez y el hambre.

Los beneficios que nos brinda esta tecnología es conocer la humedad del suelo, la cantidad de agua presente y su estado energético, determinar la presencia y duración

ISSN: 1390 -9266 – 2020 LAJC

de la humedad sobre la superficie foliar, programación de riegos y ciclos de fertilizantes acuerdos con las necesidades de la plantación, Mediciones de la cantidad de radiación solar que cae sobre el cultivo, medicines consecutivas de la cantidad de precipitación en un terreno específico, mediciones de temperatura de suelo y ambiente, mediciones de la presión barométrica, mediciones de la humedad relativa de un lote o terreno, conocer la cantidad de nutrientes disponibles en el suelo, realizar mediciones que permita conocer el grado de infección de una plaga en el cultivo, tener terrenos más productivos, cosechas más rentables, reducción de impacto ambiental y ecológico, mayor control sobre la producción en tiempo real, nos ayuda a prevenir heladas y sequías.

A. ¿Cómo funciona?

La solución de agricultura digital como servicio viene compuesta por 6 capas fundamentales para su desarrollo, que se lo describe en la figura 3.

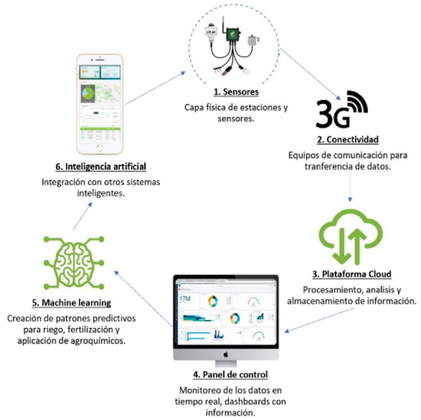


Fig. 3. Esquema del funcionamiento de la agricultura digital.

B. Plataforma módulo agricultura

El software de administración de aplicaciones con énfasis en internet de las cosas – Módulo agricultura -, donde principalmente se usa sensores con capacidad de transmisión, recolección y análisis de datos en varias actividades como: agricultura, acuacultura, avicultura, porcicultura, y en general en todo el ámbito de Internet de las cosas (IoT); ha sido desarrollado con el objetivo de incorporar una única solución con todos los medios y alternativas de administración y gestión de recursos tecnológicos existentes para la gestión empresarial en IoT.

La plataforma módulo agricultura es capaz de crear un ambiente perfectamente estructurado en su organización con la presentación de múltiples particularidades, permitiendo integrar otros dispositivos de múltiples marcas en el área de la Industria 4.0 (IoT) en una única plataforma virtual.

Destacan:

- Panel de visualización y control (Dashboard) vía web.
- Interface de configuración web.
- Multitenencia.
- Visualización de datos en tiempo real.
- Estadísticas sencillas de datos.
- Multilenguaje.
- Administración jerárquica de usuarios.
- Reportes avanzados.
- Notificaciones al buzón de correo electrónico.
- Alertas visuales.
- Capacidad de integración con otros sistemas de control/monitoreo.
- Diversidad de aplicaciones.
- Interconexión entre APIs.

C. Lectura y muestra de información de los sensores

La información recolectada por los sensores se podrá mostrar por medio de:

- Dashboards iniciales, generales para agricultores como personalizables (vía web) según la cantidad de sensores que estén leyendo información.
- Tipos de gráfico: Gráficos continuos, Barras y Circulares.
- Muestra de Gráficos seleccionables mostrando estadística de la variable, en tiempo real y pudiendo seleccionar rangos de minutos y horas (el mismo día) y fechas (comparando entre días, semanas, meses, trimestres, años).
- Muestra de gráficos estadísticos mostrando mínimo, máximo y promedio de cada variable, pudiendo seleccionar rangos de tiempo.
- Poder mostrar la foto del sensor en el interfaz, cuando se selecciona un parámetro para que muestre el gráfico.
- Poder mostrar la foto del producto de cultivo por cada estación de sensores.
- Ciertos parámetros requieren gráficos especiales, como dirección del viento en forma de brújula, presión atmosférica en forma de aguja analógica, batería del panel solar, etc.

D. Información básica en mapas GPS

Uno de los aspectos importantes de la plataforma es el nodo ubicación por GPS de las estaciones instaladas en campo como se observa en la figura 4, permite observar lo siguiente:

- Se muestra la ubicación geográfica de donde está instalado el sensor en un mapa, utilizando acceso a
- herramientas como google Earth o pudiendo cargar fotos de mapas JPG, GIF, Autocad.
- Muestra la ubicación panorámicamente de varios sets de sensores si están geográficamente cerca o en la misma zona.
- Muestra mapas regionalmente, por ciudad, provincia, país o continente si existen varios sensores conectados geográficamente separados.

Fig. 4. Instalación de sensor en cultivo de pitahaya

E. Mostrar información básica de tablas

- Muestra tablas de recolección de datos en tiempo real.
- Muestra tablas de información seleccionando solamente ciertas variables y/o cierto rango de tiempo.

F. Internet de las cosas

Un aspecto fundamental en la Industria 4.0 es el Internet de las cosas. IoT es una capa que nos permite interconectar diferentes sensores, maquinarias, equipos entre sí para una función en concreto.

En el campo de la agricultura, IoT permite que sensores, maquinarias, sistemas de riego, equipos fumigadores se puedan conectar entre sí, para optimizar procesos que ayuden a obtener una mayor producción y facilitar la tarea del agricultor en el día a día.

IoT módulo agricultura transforma los datos en productividad en cualquier cultivo, permitiendo ser mas eficiente con los datos recolectados mediante los sensores en campo, creando interacciones entre maquinarias agrícolas, creando patrones predictivos y almacenando la información en plataformas digitales.

IV. ANÁLISIS DE DATOS

Los sensores fueron colocados en el cantón Palora, Provincia Morona Santiago, Ecuador por un periodo de tiempo establecido desde el 29 de enero del 2020 hasta el 31 de marzo del presente año, donde se recolectó, analizó e interpretó la información obtenida de los sensores de suelo y medio ambiente.

A. Pluviosidad

Mediante el sensor pluviómetro se obtuvo los datos de la cantidad de lluvia que hubo en el rango de tiempo establecido y en el lote donde se colocó los sensores, esta información se la recolectó en tiempo real.

Los datos obtenidos de este parámetro fueron los siguientes: el 0 siendo el mínimo representa los días que no hubo lluvia sobre el área medida y 47.5 siendo el dato más alto, obteniendo una media inferior a 7 mm/día ilustrado en la figura 5.

ISSN: 1390 -9266 – 2020 LAJC

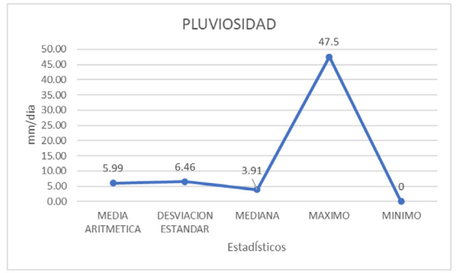


Fig. 5. Datos de la cantidad de lluvia recolecados en el sector de Palora.

B. Radiación solar

Se recolectó los datos obtenidos de la cantidad de radiación solar que hubo sobre el sector medido.

Los datos obtenidos fueron los siguientes: el 0 representa las horas que no hubo radiación solar y 2581.51 PAR siendo el dato más alto, que representa las altas radiaciones que suelen persistir en el cantón en estudio como se puede apreciar en la figura 6.

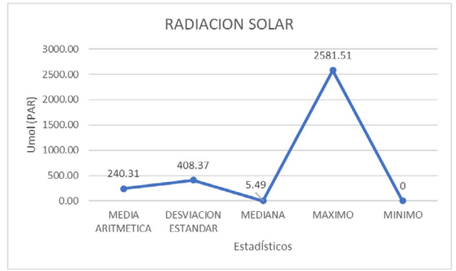


Fig. 6. Datos de la cantidad de radiación solar recolecados en el sector de Palora.

C. Humedad del suelo

Se recolectó los datos obtenidos de las continuas mediciones sobre la humedad que tenía el suelo, para conocer si el cultivo necesitaba algún suministro de agua adicional.

Los datos fueron los siguientes: el 0.17 cb siendo el mínimo representan los días que hubo muy poca humedad y 16.40 cb siendo el dato más alto. Esto nos indica que la cantidad de agua que cae a través de la lluvia permite al cultivo desarrollarse sin estrés hídricos, cabe mencionar que en el cultivo analizado no cuenta con un sistema de riego instalado, toda el agua que recibe el suelo y las plantas es por las lluvias recurrentes in situ como lo podemos observar en la figura 7.

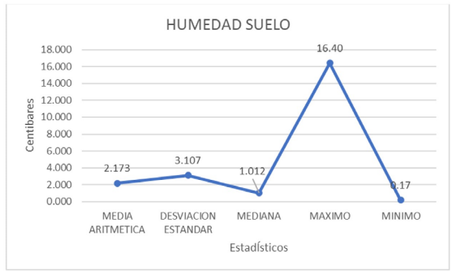


Fig. 7. Datos de la cantidad de humedad del suelo recolecados en el sector de Palora.

D. Temperatura ambiental

Se recolectó los datos obtenidos de las mediciones sobre la temperatura ambiental sobre el sector de medición.

Los datos fueron los siguientes: el dato 13.61 °c fue el más bajo y representa la temperatura más baja y el 35.09 °c fue el dato más alto siento la temperatura máxima que se dio en el sector de medición de cultivo. La temperatura es un parámetro influyente en el desarrollo del cultivo, afecta directamente en la transpiración y humedad de este como lo podemos visualizar en la figura 8.

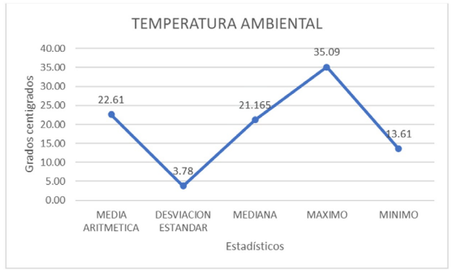


Fig. 8. Datos de la temperatura ambiental recolecados en el sector de Palora.

V. CONCLUSIONES

El cantón Palora presenta una gran cantidad de mm/día de precipitaciones, razón por la cual el cultivo de pitahaya se desarrolla sin suministro de agua adicional. La cantidad de lluvia que cae sobre el cultivo permite satisfacer las necesidades de este para su desarrollo.

El cultivo de Pitahaya en el cantón Palora, tiene una constante exposición de rayos solares (PAR) durante el día, teniendo un pico en las horas del mediodía, 11h00 a 14h00, que le permite a la planta engrosar el fruto y tener una adecuada fotosíntesis.

Los datos obtenidos evidencian que la humedad de suelo siempre estuvo en un rango óptimo de capacidad de campo, con un promedio inferior a 5 centibares.

La temperatura ambiental es un influyente directo en el aumento o mantenimiento de la humedad del suelo, mientras más temperatura y radiación solar, la humedad del suelo siempre aumenta, por tal motivo el cultivo requiere agua para no sufrir ningún estrés.

El uso de la tecnología en agricultura es fundamental para conocer los datos reales en un cultivo, poder tomar decisiones al instante, disminuir costos de mano de mano de obra, costos de energía, agua y de aplicaciones de insumos agrícolas en todo el ciclo.

La plataforma módulo agricultura, permite realizar análisis estadísticos, con tablas y gráficos, para poder tomar correctivos durante la campaña actual o la siguiente, creando patrones predictivos que nos permitan prevenir heladas, enfermedades, virus, plagas y hasta largas sequías en épocas de temporada seca.

AGRADECIMIENTO

El autor agradece a todo el grupo humano que trabaja día a día en la empresa TELCOMBAS S.A. sin ellos el trabajo no hubiera sido factible realizarlo.

Segundo agradece a la finca Procell de Palora, por abrirnos las puertas de sus instalaciones y confiar en el uso de nuevas tecnologías para la producción de sus cultivos.

Finalmente, agradece a Christian Bascompte CEO de TELCOMBAS S.A. por impulsar este proyecto y siempre tener la mentalidad de no quedarse en la zona de comfort, sino siempre apuntar hacia la innovación y el cambio.

ISSN: 1390 -9266 – 2020 LAJC

VI. REFERENCIAS

[1] P. Esquivel, Y. Araya, “Características del fruto de la pitahaya (hylocereus sp.) y su potencial de uso en la industria alimentaria,” Revista Venezolana de Ciencia y Tecnología deAlimentos, vol. 3, pp. 114, 2012.

[2] V. Fuentes, “Etnobotánica de cactaceae en cuba,” Instituto de Investigaciones en Fruticultura Tropical, Ministerio de la Agricultura, C. Habana, pp 23, 2012.

[3] GAP Municiapal Palora, [Online]. Available: http://www.palora.gob.ec/web/index.php/2016-07-06-18-01-03/ubicacion#:~:text=El%20cant%C3%B3n%20Palora%20se%20encuentra,poder%20utilizar%20Mapas%20de%20Google. [Accessed: Nov.17, 2020].

[4] Ministerio de Agricultura Ganaderia y Pesca (MAG), “Primer censo de pitahaya,” [Online]. Available: https://www.agricultura.gob.ec/en-palora-morona-santiago-se-realiza-el-primer-censo-de-pitahaya/ [Accessed: Nov.17, 2020].

[5] G. Orrico, “Respuesta de la pitahaya amarilla(Cereus triangularis L.) a la aplicación complementaria de dos fertilizantes en tres dosis,” Universidad Central del Ecuador. Quito – Perú, pp 3, 2013.

[6] Paraiso. 2013. “Ecofinsa frutas ecuatorianas de calidad,” [Online]. Available: http:www.ecofinsa.com/pitahaya [Accessed: Nov.17, 2020].

[7] C. Santacruz, C. Santacruz, C. y E. Huerta, “Agroindustrialización de Pitaya,” Bemérita Universidad Autónoma de Puebla- México, pp 23, 2009.

[8] L. Penelo, “Pitaya: propiedades, beneficios y valor nutricional,” Revista la Vanguardia, 2020. [Online]. Available: https://www.lavanguardia.com/comer/materia-prima/20180720/45956036053/pitaya-fruta-propiedades-beneficios-valor-nutricional.html. [Accessed: Nov.17, 2020].

[9] SN, “ Pitahaya Amarilla,” Revista Frutas exoticas 10, 2019. [Online]. Available: https://frutasexoticas10.com/pitaya/pitaya-amarilla/ [Accessed: Apr.18, 2020].

AUTHOR

Ángel Llerena Zambrano

Ingeniero Agropecuario, y Master en Tecnología Agroambiental para una Agricultura Sostenible por la Universidad Politécnica de Madrid. Product Manager IoT de la empresa Telcombas S.A. Manejo de distintos cultivos tropicales mediante tecnología IoT para el aumento de producción. Investigador de proyectos relacionados con la aplicación de ozono para el control de la Sigatoka Negra en Ecuador. Amplia experiencia en el análisis de información recolectada a través de sensores con tecnología IoT.

ISSN: 1390 -9266 – 2020 LAJC

A. Llerena-Zambrano, "Agricultura digital en el cultivo de Pitahaya", Latin-American Journal of Computing (LAJC), vol. 7, no. 2, 2020.

LATIN-AMERICAN JOURNAL OF COMPUTING (LAJC), Vol VII, Issue 2, December 2020

Anomaly Detection Under a Cognitive Security Model

Detección de Anomalías Bajo un Modelo de Seguridad Cognitiva

ARTICLE HISTORY

Received 01 October 2020
Accepted 16 October 2020

Jonathan Herrera
Departamento de Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
jonathan.herrera01@epn.edu.ec

Roberto Omar Andrade
Departamento de Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
roberto.andrade@epn.edu.ec

Miguel Flores
Departamento de Matemáticas
Escuela Politécnica Nacional
Quito, Ecuador
miguel.flores@epn.edu.ec

Susana Cadena
Facultad de Ciencias Administrativas
Universidad Central del Ecuador
Quito, Ecuador
scadena@uce.edu.ec

Anomaly Detection Under a Cognitive Security Model

Detección de Anomalías Bajo un Modelo de Seguridad Cognitiva

Jonathan Herrera
Departamento de Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
jonathan.herrera01@epn.edu.ec

Roberto Omar Andrade
Departamento de Ciencias de la Computación
Escuela Politécnica Nacional
Quito, Ecuador
roberto.andrade@epn.edu.ec

Miguel Flores
Departamento de Matemáticas
Escuela Politécnica Nacional
Quito, Ecuador
miguel.flores@epn.edu.ec

Susana Cadena
Facultad de Ciencias Administrativas
Universidad Central del Ecuador
Quito, Ecuador
scadena@epn.edu.ec

Abstract — Cybersecurity attacks are considered among the top five of risks worldwide, according to the World Economic Forum in the year 2019. This context has generated the need to improve the tasks of cybersecurity defense in organizations. Improving the effectiveness in executing a cybersecurity task requires three pillars: people, processes and technologies. The proposal in this work is to analyze the integration of these three components as a strategy to improve the effectiveness of the execution of operational tasks in cyber defense, specifically the detection of anomalies. Based on the foundation that: cybersecurity operational tasks carried out daily by analysts require the use of cognitive processes, and that the use of techniques based on technologies such as machine learning, data mining and data science have generally been used to automate cybersecurity tasks, we have considered the use of cognitive security, as a strategy to improve the anomaly detection process, taking into account the cognitive processes and skills that are executed by the security analyst.

Keywords — cyber-defense, cognitive security, cybersecurity.

Resumen — *Los ataques de ciberseguridad están considerados entre los 5 principales riesgos alrededor del mundo, de acuerdo al World Economic Forum en el año 2019. Este contexto ha generado la necesidad de mejorar las tareas de defensa de ciberseguridad en las organizaciones. Mejorar la efectividad en ejecutar una tarea de ciberseguridad requiere tres pilares: personas, procesos y tecnologías. El propósito de este trabajo, es analizar la integración de estos tres componentes como una estrategia para mejorar la efectividad de la ejecución de tareas operacionales de ciberdefensa, específicamente la detección de anomalías. Basados en el fundamento de: que las tareas operacionales de ciberseguridad llevadas a cabo diariamente por analistas, requieren de procesos cognitivos, y que el uso de técnicas basadas en tecnologías como el aprendizaje de máquina, la minería de datos y la ciencia de datos han sido usadas generalmente para automatizar las tareas de ciberseguridad como la detección de anomalías, hemos considerado el uso de la seguridad cognitiva, como una estrategia para mejorar el proceso de detección de anomalías, teniendo en cuenta los procesos y habilidades cognitivas que son ejecutadas por el analista de seguridad.*

Palabras clave — *ciber-defensa, seguridad cognitiva, ciberseguridad*

ISSN: 1390 -9266 – 2020 LAJC

I. INTRODUCTION

The development of computer applications and emerging technologies, such as smart cities or industry 4.0, have optimized the technology services provided by organizations around the world. Additionally, the improvement of decision-making processes in real time has become a challenge for security managers. Furthermore, cyber security problems have been increasing constantly; attacks on system availability, information theft and loss of privacy have risen in recent years, according to the World Economic Forum [1].

In this context, the need to improve the cognitive skills of security analysts, and the use of technological tools to support cyber operations has increased. From our perspective, a direct relationship between the development of technological solutions and the skills of security analysts is important. Having an effective tool, but lacking a person capable of handling it, would limit the effectiveness of said tool, and on the other hand, an analyst with extensive experience who does not have effective tools would be limited in his or her ability to perform cybernetic operational tasks.

In this study, it is our interest to analyze the importance of cognitive security regarding anomaly detection. Based on the literature review carried out in a previous work [2], "Self-Awareness as Enabler of cognitive Security", cognitive security is considered as: the ability to generate cognition in order to take decisions effectively in real time, by either a human or a computational system. This ability is based on the perception generated by the system from its environment and the knowledge about itself, which is obtained from the analysis of any type of information, structured or unstructured, by using artificial intelligence techniques and data analysis. Therefore, the system can emulate the human thought process for continuous learning, decision making and, ultimately, security analysis.

Given the fact that we intend to work with enormous amounts of data, we propose the use of the Elastic Stack (ELK). ELK is a set of tools that aim to help improve the indexation, searching and manipulation of the data [3]. In this study, we implement the ELK stack in order to index and analyze the data obtained from the IoT-23 dataset, which were downloaded directly from [4]. This data is analyzed in order to asses the connection and future development of a cognitive model, either supervised or unsupervised, which could be used to classify the data in a more reliable way. The results obtained showed a clear distinction between the behavior of the malicious traffic and the benign traffic, which facilitates the development of a future cognitive model based on the data.

II. THEORETICAL FOUNDATION

There are a set of security operational tasks that are developed daily by security analysts and that requires of the use of cognitive skills for their execution. These tasks were indicated by IBM at the RSA conference in 2017 [5]. On previous related work, we had grouped these tasks on base of cognitive processes and the Observe–Orient–Decide–Act (OODA) cognitive model, proposed by Breton (See Table I, Table II and Table III) [6-7].

TABLE I. OODA COGNITIVE PHASE AND COGNITIVE PROCESS

Phase	Process
Observe	Feature matching /Perception
Orient	Mental models / Comprehension
Decide	Evaluating / Projection

TABLE II. COGNITIVE PROCESS AND ITS ATTRIBUTES.

Process	Attribute
Perception	Identification of relevant data
Comprehension	Interpretation of data
Projection	Prediction of future events

The first two cognitive tasks "Review incident data" and "Review the events by aspect of interest" require the cognitive skill of perception by security analyst. The third task "Pivot in the data to find atypical values, or outliers" requires the cognitive process called comprehension. One of the daily operations carried out by security analysts, and related with these three tasks, is anomaly detection, i.e., the analyst's ability to identify outliers that could be possible security attacks, based on spikes in data traffic or by connections from uncommon services. This detection could allow

the security analyst to take the appropriate actions, and reduce the impact of the attack.
Within cybersecurity, one of the concerns of security managers are anomalies, which are defined as the detection of surprising or unusual events [5]. There are several techniques to detect anomalies, which use a range of different methods, however, it should be considered that, when the malicious actions are caused by perpetrators, the abnormal observations tend to be adapted in order to appear normal. Another major problem is the availability of labeled data, which is needed for training and validating the computational models. To determine an anomaly, several factors should be considered such as: the nature of the input data (object, record, point, vector, pattern, event, case, sample, observation or entity), the availability or not of labels, as well as the limitations and requirements induced by the domain of the application [6].

TABLE III. COGNITIVE PROCESS RELATED TO CYBER-ATTACKS

Cybersecurity operations tasks	Cognitive process
Review incident data	Perception
Review the events by aspects of interest	Perception
Pivot in the data to find atypical values or outliers	Comprehension
Expand the search to find more data	Projection
Investigate the treath to develop experience	Comprehension
Discover new treaths	Projection
Determine indicators of commitment in other sources	Comprehension
Apply intelligence to investigate the incident	Projection
Discover potentially infected IPs	Comprehension
Qualify the incident based on the knowledge generated while investiganting the threat	Comprehension
Prescriptive analysis based on the profile of the attack	Comprehension
Analysis of the lessons learned, based on the dispersion map of the attack	Comprehension

III. ANOMALY DETECTION BASED ON COGNITIVE SECURITY

The objective of this work is to define the anomaly detection process by the security analyst, in order to translate it to a cognitive security model. The first cognitive process, used by an analyst for the detection, is the perception. The analyst must have the ability to detect outliers, by reviewing the data generated in the ecosystem. Based on the three steps proposed by [8], we propose in Figure 1, an anomaly detection process based in a cognitive model.

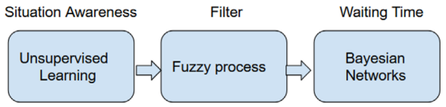


Fig. 1. Anomaly detection process based on a cognitive model

The security analyst first establishes an awareness of the situation. According to [9], unsupervised models are more

Riveiro mentions a five-phase process related to the anomaly detection process [8]:

1. Overview: continuous traffic control in real-time.
2. Filter: define if something is abnormal (make a judgment based on their experiences).
3. Waiting Time: in which the event is observed in order to evaluate its behavior.
4. More detail: the situation is analyzed in more detail.
5. Taking-action: define the best responsive action.
   The first

The first step according to [8], is establishing the potentially dangerous situation, where the analyst should compare it, and update it, according to what would be the normal situation in the supervised zone. The second step correspond to narrowing the set of items, where the analyst zooms in and out the data to detect anomalous behavior, comparing it with real-time information. In this step, [8] suggests the use of data-mining techniques to decrease the time needed to identify anomalous situations. The third step is critical, because the analyst leaves the current traffic, in order to evaluate the status of the situation. This step is stressful for the analyst, due to the potential increase of traffic, or any impact in the services of the supervised zone. These three steps, defined by [8], require the analysts' cognitive processes, which we have grouped together in this work within the cognitive process called "perception".
Increasing the analyst's cognitive skills can be carried out by several lines of action:

- Training,
- Experience gained from work,
- Technological solutions, or
- Cognitive security

ISSN: 1390 -9266 – 2020 LAJC

efficient and appropriate for the detection of abnormalities, compared to human analysts. The use of supervised algorithms requires the establishment of labels, and continuous training by a security analyst. However, new security attacks may not be identified by the analyst, which would limit the effectiveness of the algorithm. In this context, unsupervised algorithms can have a greater advantage.

A security analyst requires three cognitive functions in order to execute anomaly detection:

1. The ability to detect patterns and outliers from a dataset.
2. The ability to identify the time when an event occurred based on timestamps.
3. The ability to establish a geographical or spatial locality from where the attack was originated.

So, spatial and temporal reasoning are essential in the field of cybersecurity. According to [10], temporal and spatial representations are not independent between them, and different modalities are sensitive to the processing of time and space. [10] analyzes the hypotheses on the symmetric and asymmetric relationships of temporal and spatial information, and how they affect the decision-making process. In his study, he mentions that the relationship between these attributes can affect the time taken to make a judgement. Additionally, he mentions that visual analysis is more sensitive to space information that to temporal information.

In Figure 2, we show some of the attributes that could be considered as part of the temporal reasoning done by the security analyst, in order to perform an anomaly detection process. Based on the arguments of the cognitive processes proposed by [10], the use of algorithms must consider the space-time attributes, in order to improve the duration and effectiveness in the decision-making process. This is particularly important for a security analyst, when trying to identify anomalies. Additionally, the scheme using unsupervised algorithms could be hybrid, given the fact that there exists a sufficiently wide range of algorithms that can be used for this context. In Figure 3, we present an overview of some unsupervised algorithms, which could be used for space-temporal analysis in anomaly detection, among cybersecurity domains.

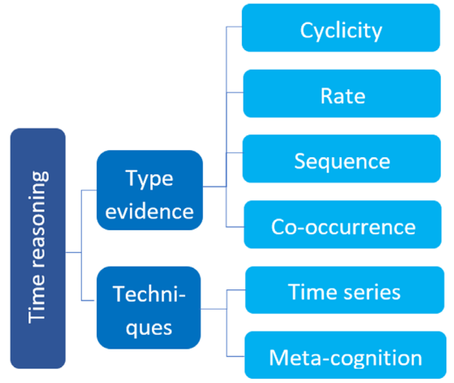


Fig. 2. Temporal Reasoning in cybersecurity anomaly detection

Some unsupervised algorithms have been used in anomaly detection before. For example, hierarchical k-means algorithms improve the clustering performance in large datasets [11]. Additionally, partition algorithms allow to reduce the complexity of time and space produced by hierarchical density [12]. There are also grid-based algorithms, which allow the detection of frequent spatial patterns [13]. These grid structures, that use space partitioning that converts space into smaller intervals, help in reducing computational overhead. Finally, in density-base clustering data, objects are categorized according to their regions of density, connectivity and boundaries [14].

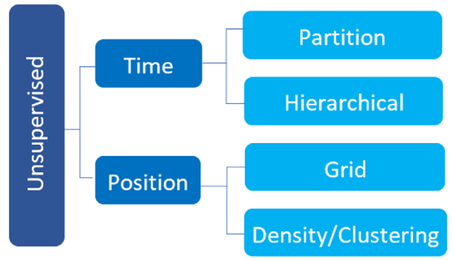


Fig. 3. Unsupervised algorithms for anomaly detection

The second step, according to [8] for anomaly detection is related to the filtering process. Anomaly detection in this step is based on the analyst's experience, so there is a high degree of subjectivity. Furthermore, the filtering process requires the processing

of collected data, including their cleaning and profiling; therefore, is common in this type of process to select a methodology such as CRISP-DM, which has been widely used in Data-Mining projects. In this study, we have established the premise that, it is not feasible for the security analyst to have knowledge of all possible attacks, and that there are new attack vectors every day; the security analyst, therefore, starts from a state of uncertainty and lack of relevant information. From this point, the security analyst must build the necessary knowledge for decision making.

Regarding uncertainty, [15] mentions that uncertainty is a property of human in his/her mental processes. In this context, cognitive uncertainty is caused by the incompleteness of the important knowledge required (vague events), where fuzziness is also included as a type of non-statistical uncertainty. [15] also mentions that, categorization, is an essential function of the cognitive system when performing important processes, such as reasoning and problem solving. She proposes a fuzzy membership function for categorization, where the function measures the degree of similarity of different objects. We can use fuzzy techniques to reduce the subjectivity of the security analysis. The fuzzy techniques could measure the relationship between two vague events: when an attack occurs (time), and the source of the attack (space). So, a fuzzy technique must be aligned with the temporal-spatial principle.

In the third step, there is a need to reduce the waiting time and select the best option, considering most of the possible scenarios. The use of Bayesian networks, with a cause-effect scheme, could support a security analyst in order to help him/her consider better alternatives. Additionally, Bayesian networks are effective while modelling large datasets, where spatial and temporal information might be included. Furthermore, the Integrated Nested Laplace Approximations (INLA) approach, is a computationally effective and an extremely powerful alternative to Monte Carlo (MCMC) methods.

IV. EXPERIMENTATION

The architecture, implemented for this study, is made up of three nodes. These 3 nodes have specific functions and will be known from now on as "collector", "index" and "reporter". The "collector" node has an Intel (R) Xeon (R) E5-2640 v4 2.40GHz processor, 4GB of DDR4 ECC memory and a 200GiB NUTANIX VDISK disk. The "index" node has the same processor and memory characteristics, with the same disk model, but with 500GB capacity. Similarly, in the "reporter" node, there are the same characteristics in processor and memory, with storage of 100 GB. All three nodes are running the Ubuntu 18.04.4 operating system. Additionally, all the nodes are connected through an Ethernet network, as shown in Figure 4, with a firewall that only allows the passage for port 22, to be able to connect using the SSH protocol. The functions of each node are differentiated for each of the components of the ELK stack. In this way, the "index" node is in charge of keeping Elasticsearch services running, indexing the data and searching for them. The "collector" node is in charge of separating, organizing and coding the information for its correct indexing within the "index" node. Finally, the "reporter" node is in charge of keeping the Kibana service running, to allow access and corresponding visualization of the data that are indexed in Elasticsearch. This node is in charge of maintaining a cache with the data that need to be shown in each query, in order to facilitate viewing and searching in real time.

To allow the visualization of the Kibana service from a computer external to the network, the "reporter" node has been provided with a public IP address, where the ports 80 and 443 are open to receive requests. The aforementioned ports are routed through a proxy, implemented using the Nginx service, which allows us to redirect incoming traffic to the corresponding Kibana port This port (5600) has been arbitrarily chosen for communication, the default port (5601) would also have the same functionalities.

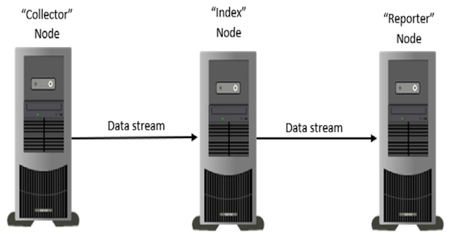


Fig. 4. Big Data Architecture

ISSN: 1390 -9266 – 2020 LAJC

A. Configuration

Los algoritmos de OCR permiten convertir el texto en una imagen a caracteres (códigos de 8 bits, como los representados en tablas ASCII). El motor o algoritmo OCR adoptado es el motor Tesseract OCR.

Index node

In the "index" node, Elasticsearch 7.9.0 was installed as indicated in [16], through a Debian package, which was downloaded directly from the Elastic servers. Once the node was installed, we proceeded to configure the elasticsearch.yml file, which is located in the / etc/elasticsearch directory. In this file, the name of the cluster, the name of the node, the address for the data, the address for the records and the port where it will receive HTTP requests were configured. Additionally, x-pack was configured, following the steps indicated in [17]. For this purpose, the variable xpack.security.enabled was set to true in the elasticsearch.yml file, in order to enable the x-pack configuration for within the Elasticsearch instance. The x-pack service contains essential users included; whose respective passwords were configured by running the elasticsearch-setup-passwords service. This service was located in the elastic installation folder, and it was run using the interactive option.

Reporter Node

In the "reporter" node, the Kibana 7.9.0 service was installed, following the steps indicated in [18]. Similarly, a Debian package was used, which was downloaded from the Elastic servers. Once Kibana was installed, the kibana.yml file was configured, which is located in the /etc/kibana folder. The options configured in this file were: the server port, the host address, the elasticsearch host address, the elasticsearch listening port, the existing username of "kibana" for elasticsearch and the password that was configured in a previous step. The Kibana service was started, and kept running in background mode.

Collector Node

The Logstash 7.9.0 service was installed in the "collector" node, following the steps specified in [19]; likewise, the installation was carried out with the use of a Debian package, downloaded from the Elastic servers. Once the installation was ready, we proceeded to configure only the location of the data in the logstash.yml file, since the rest is configured in the configuration file of the corresponding pipeline. Additionally, in order to connect Logstash to Elasticsearch using x-pack, a specific user was first configured for Logstash, as specified in [19]. This user was configured using Kibana's interface, where an Index Pattern called logstash- and a user role called "logstash_writer" were created, with the following privileges:

- Cluster: "monitor" and "manage_index_templates"
- Index: "write", "create", "delete" and "create_index" in the indexes that meet the pattern logstash- *

Finally, a user named logstash_internal was created, with the role of logstash writer, and a password was configured for its access.

B. Data Indexing

The data that were used belongs to the IoT-23 dataset, which is obtained from PCAP files and transformed into a connection log by using Zeek, which gives them a high-level format. These files were downloaded directly from the repository mentioned in [4]. In order to index them, a .conf file was used, located in the / etc/logstash/conf.d/ folder; the configuration of this file was done according to what is indicated in the documentation for logstash 7.9.0 [20]. In the input section, the location of the x-pack files within the file plugin was configured, which is part of the logstash plugins and is specified in [20]. Additionally, the start_position variable was set to "beginning" and the "sincedb_path" variable to "/dev/null". This was done so that logstash reads the entire file instead of using the default configuration, which only reads the last lines and monitors changes.

The filter section of the configuration file was started by checking the received rows with "if [message] = ~ / ^ # /", which then executes the "drop" plugin, specified in [21]; this is done to filter those lines that are comments in the obtained record. Next, the Grok plugin was used to filter the rows and separate the data into the corresponding attributes, assigning each attribute the corresponding value as indicated in the header of the log file. This Grok filter was tested using the filter test function that is available among the Kibana plugins. Additionally, the "translate" plugin was used to obtain an additional attribute, which better explains the connection status from the codes that are given in the file. Later, making use of several conditionals, the values of '-' were replaced in the following attributes: "id. orig_p", "id.resp_p", "orig_bytes", "resp_bytes", "missed_bytes", "orig_pkts", "orig_ip_bytes", "resp_pkts", "resp_ip_bytes " and "duration". Additionally, the aforementioned values were converted to "integer" using the "mutate"

plugin, specified in [21], with the exception of the "duration" attribute, which was transformed to "float". Finally, the last plugin used in this section is the date plugin, which is detailed in [21], where it was indicated that the time value is in the "ts" field, and that it is formatted in UNIX time.

In the output section, the "Elasticsearch" plugin was used, which is detailed in [22]. which was configured with the address of the "index" node and the Elasticsearch port. In this section, the user created previously for the use of Logstash was entered, along with its respective password. Additionally, in this section the location of a "template" that should be used for the creation of the index was indicated, specifying its name and that it should not be overwritten. In this template, which is structured as indicated in [23], we proceeded to specify the "mapping" of the index fields. This mapping was used to specify the data type for all the values that were previously encoded in numeric format. The Logstash service was then started using the "sudo systemctl start logstash" command, to run in background mode. Finally, the index was modified through the Elasticsearch API to reduce the number of replicas to zero, because there is only one node working with Elasticsearch and there is no possibility of implementing replicas of it.

V. RESULTS AND DISCUSSION

Once the data had finished loading into the index, an Index Pattern was created in Elasticsearch from Kibana. This pattern was used to verify the loaded data. As can be seen in Figure 5, the loaded data has been correctly indexed, with the format established in the template that was previously defined. With this Index Pattern, a dashboard was created, allowing a clearer view of the data that was indexed. To create the dashboard, the Kibana tool was used, and six visualizations were obtained.

Fields (54) | Scripted fields (0) | Source filters (0)

Search

Name	Type
@timestamp	date
@version	string
_id	string
_index	string
_score	number
_source	_source
_type	string
conn_state	string
conn_state.keyword	string
conn_state_full	string

Rows per page: 10

Fig. 5. Data according to Index pattern.

In Figure 6, the first visualization can be seen, which consists of the average size of a request and a response according to the type of traffic. It can be clearly seen that there are marked differences between benign and malicious traffic. In the case of the request, this tends to be smaller for benign traffic; while the answer is larger for the malicious traffic. This can be easily interpreted because the attackers tend to request information from the device that they are targeting in order to understand its vulnerabilities.

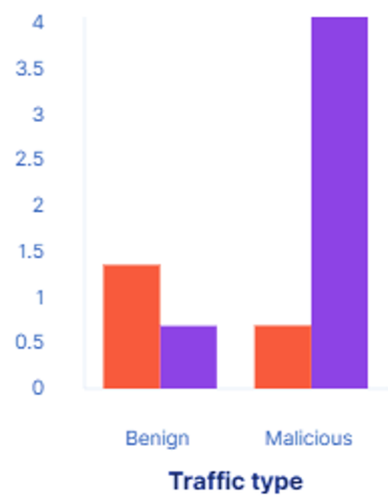


Fig. 6. Average data size according to traffic

Figure 7, allows us to appreciate the ports at which the malicious traffic is being directed. As it can be seen, the traffic tends to attack specific ports of some well-known protocols, such as telnet and HTTP. This is obviously done, in order to try to obtain access via these ports since they tend to be open in most cases. In contrast, in Figure 8, a huge difference can be seen in the ports that are being targeted by the benign traffic. Since this traffic has legitimate petitions, that are used to perform communications between the IoT devices, this clear difference was expected to be seen, according to the type of traffic.

ISSN: 1390 -9266 – 2020 LAJC

The data obtained from the IoT dataset have allowed us to appreciate the differences between the behavior of benign and malicious traffic more easily. As it was previously seen, the differences in the traffic is clear enough to perform a detection by a security analyst only by visualizing the behavior of the data. Based on this principle, a Bayesian Network could be developed in order to detect the anomalies in the traffic. One of the obvious rules that could be used, would be a detection based on the size of the petition, relative to the size of the answer, in order to detect a possible attack that tries to gather information of the system.

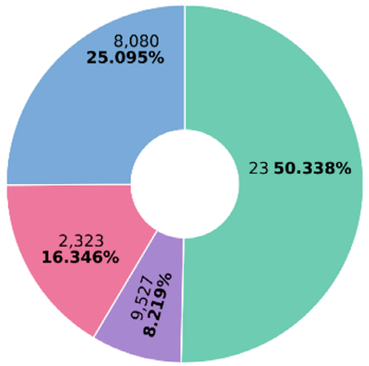


Fig. 7. Ports targeted by malicious traffic.

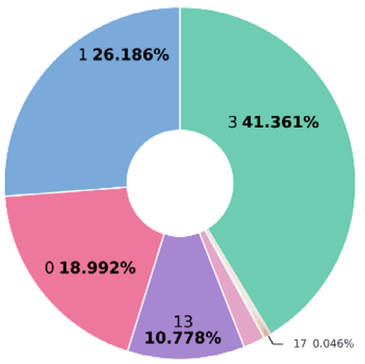


Fig. 8. Ports targeted by benign traffic.

Figure 9 shows the capabilities of ELK to display an anomaly timeline, created in base of multiple metrics. For instance, count of events versus IP address. This figure is also allowing us to identify the time of a day at which an anomaly is more likely to appear. Therefore, a system could be deployed to alert analysts of incoming traffic during those specific times of the day. The analyst could, consequently, prepare itself for a more focused and intensive analysis of the incoming traffic, since it has a higher probability of being a possible threat, due to the time of the day at which it is currently being performed. Additionally, the data clearly shows a difference in the ports that are being targeted by the malicious traffic, compared to the ports targeted by benign traffic. This difference is so prevalent that most security analysts already know which ports need to be secured, since those ports are more likely to be the target for future attacks. This data, therefore, allow analysts to protect the most vulnerable ports, and prevent them for the future, in order to focus their attention in the most vulnerable parts of the system.

Fig. 9. Anomaly timeline based on multiple metrics.

VI. CONCLUSION

Currently, not only computers generate data, but IoT solutions also present an additional challenge by having objects connected to the internet, such as sensors and appliances (televisions, refrigerators or cars), which are capable of generating data.

The substantial difference from our point of view of cognitive security as a cybersecurity strategy, versus other strategies, is the augmentation of the analysts' cognitive skills. Coupling technological, and data science solutions, to the cognitive process can generate a bidirectional contribution to the technological tool or algorithm, because it can be better trained and configured. Additionally, the analyst also obtains a bidirectional contribution, because they will get support in the development of their own operational tasks.

The efficiency at executing tasks in cybersecurity, depends of the cognitive processes made by a security analyst. Additionally, the detection of anomalies also requires a cognitive process, and its effectiveness depends mostly on the degree of expertise that the analyst has. In this study, we have tried to highlight the importance of spatial-temporal reasoning, as one of the cognitive skills that must be developed by analysts to improve the anomaly detection processes.

Based on the spatial-temporal reasoning, we have proposed the use of data-science solutions such as unsupervised machine learning algorithms, fuzzy techniques and Bayesian networks, which can improve anomaly detection processes. In this study we wanted to highlight the importance of cognitive security, by integrating the point of view of the analyst's cognitive processes with the technological and analytical solutions available to support them.
The ELK stack has great capabilities for the analysis and indexing of data. In addition, it allows searching and storing data very easily, and has enormous possibilities for the analysis of large amounts of data. The use of this stack for the analysis of traffic data in IoT devices, has allowed us to improve the visualization of a huge number of records in a very fast time. The Kibana tool has great capabilities, which can be used to display large amounts of data in an intuitive way; with this tool, it has been possible to create visualizations with great potential, and that take very little time to update, thanks to the optimized operations performed in the indexes at Elasticsearch. Additionally, the implementation of Logstash increases the capabilities of the ELK stack, by allowing it to perform the indexing of the data in a simple way. Logstash functions to perform the reading, filtering and writing of information, allow the processing of any type of record easily and quickly. Finally, the use of the Grok plugin for structuring previously unstructured files, is the main tool that allows encoding and organizing the information in the records.

Future works on this field could be focused in the development of an automated system, which would use the data collected for this study to train an unsupervised anomaly detection algorithm. This algorithm could use various techniques, including Isolation Forest, Clustering and Histogram based algorithms to perform an automatic detection of anomalies, in order to help aid the security analyst in his work. Additionally, the relative simplicity of the previously mentioned algorithms during the deployment phase, will make it easy to perform real time intrusion detection, without causing any significant overhead in the system. Therefore, an automated system deployed to perform anomaly detection will efficiently use the resources and, hopefully, reduce the workload of a security analyst in a significant manner, without losing efficiency in detecting possible intrusions.

VII. REFERENCES

[1] World Economic Forum®, "The Global Risks Report 2019", The Global Risks Report, 2019. [online] Geneva: World Economic Forum. Available at: <http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf> [Accessed 28 September 2020].

[2] R. Andrade and J. Torres, J. "Self-Awareness as an enabler of Cognitive Security", IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018.

[3] Elasticsearch B.V., "Elasticsearch: The Official Distributed Search & Analytics Engine", 2020. [Online]. Available: https://www.elastic.co/elasticsearch/. [Accessed: 28- Sep- 2020].

[4] A. Parmisano, S. Garcia and M. Erquiaga, "Stratosphere Laboratory", A labeled dataset with malicious and benign IoT network traffic, 2020. [Online]. Available: https://www.stratosphereips.org/datasets-iot23. [Accessed: 28- Sep- 2020].

ISSN: 1390 -9266 – 2020 LAJC

[5] IBM, "Applied cognitive security complementing the security analyst.", 2017. [Online]. Available: https://www.rsaconference.com

[6] R. Breton and R. Rousseau, "The c-ooda: A cognitive version of the ooda loop to represent c2 activities. topic: C2 process modelling," 03 2019.

[7] M. D. Mumford, E. Todd, C. Higgs, and T. Mcintosh, "Cognitive skills and leadership performance: The nine critical skills," The Leadership Quarterly, vol. 28, 11 2016.

[8] Riveiro, M., Falkman, G., Ziemke, T., & Kronhamn, T. "Reasoning about anomalies: a study of the analytical process of detecting and identifying anomalous behavior in maritime traffic data", Proceedings of SPIE - The International Society for Optical Engineering, 2009.

[9] J. Ma and S. Perkins, S., "Time-series novelty detection using one-class support vector machines", Proceedings of the International Joint Conference on Neural Networks, 2003. doi:10.1109/ijcnn.2003.1223670

[10] J. Loeffler, R. Cañal-Bruland, A. Schroeger, J. W. Tolentino-Castro, and M. Raab, "Interrelations between temporal and spatial cognition: The role of modality-specific processing", Frontiers in Psychology, 9, Article 2609, 2018. https://doi.org/10.3389/fpsyg.2018.02609 T. S.

[11] Xu, H. D. Chiang, G. Y. Liu, and C. W. Tan. Hierarchical k-means method for clustering large-scale advanced metering infrastructure data. IEEETransactions on Power Delivery, 32(2), 609–616, 2017.

[12] S. Dhandapani, G. Gupta, and J. Ghosh. Design and implementation of scalable hierarchical density based clustering (Doctoral dissertation, University ofTexas), 2010.

[13] P. Berkin. A survey of clustering data mining techniques, in: J. Kogan, C. Nicholas and M. Teboulle (Eds.), Grouping Multidimensional Data: RecentAdvances in Clustering, pp. 25–71, 2006.

[14] D. Pascual, F. Pla, and J. S. Sanchez. Nonparametric local density-based clustering for multimodal overlapping distributions, in: Proceedings of the 7IntligentDataEngineeringandAutomated Learning (IDEAL), Burgos, Spain, pp. 671–678, 2006.

[15] C. M. Varachiu and N. Varachiu, "A fuzzy paradigm approach for the cognitive process of categorization," Proceedings First IEEE International Conference on Cognitive Informatics, Calgary, Alberta, Canada, 2002, pp. 229-232, doi: 10.1109/COGINF.2002.1039302.

[16] Elasticsearch B.V., "Installing Elasticsearch | Elasticsearch Reference [7.9] | Elastic", Elastic.co, 2020. [Online]. Available: https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html. [Accessed: 28- Sep- 2020]

[17] Elasticsearch B.V., "Configuring security in Elasticsearch | Elasticsearch Reference [7.9] | Elastic", Elastic.co, 2020. [Online]. Available: https://www.elastic.co/guide/en/elasticsearch/reference/7.9/configuring-security.html. [Accessed: 28- Sep- 2020].

[18] Elasticsearch B.V., "Install Kibana | Kibana Guide [7.9] | Elastic", Elastic.co, 2020. [Online]. Available: https://www.elastic.co/guide/en/kibana/current/install.html. [Accessed: 28- Sep- 2020].

[19] Elasticsearch B.V., "Installing Logstash | Logstash Reference [7.9] | Elastic", Elastic.co, 2020. [Online]. Available: https://www.elastic.co/guide/en/logstash/current/installing-logstash.html. [Accessed: 28- Sep- 2020].

[20] ElasticSearch B.V., "Input plugins | Logstash Reference [7.9] | Elastic", Elastic.co, 2020. [Online]. Available: https://www.elastic.co/guide/en/logstash/current/input-plugins.html. [Accessed: 28- Sep- 2020].

[21] Elasticsearch B.V., "Filter plugins | Logstash Reference [7.9] | Elastic", Elastic.co, 2020. [Online]. Available: https://www.elastic.co/guide/en/logstash/current/filter-plugins.html. [Accessed: 28- Sep- 2020].

[22] Elasticsearch B.V., "Output plugins | Logstash Reference [7.9] | Elastic", Elastic.co, 2020. [Online]. Available: https://www.elastic.co/guide/en/logstash/current/output-plugins.html. [Accessed: 28- Sep- 2020].

[23] Elasticsearch B.V., "Index templates | Elasticsearch Reference [master] | Elastic", Elastic.co, 2020. [Online]. Available: https://www.elastic.co/guide/en/elasticsearch/reference/master/index-templates.html. [Accessed: 28- Sep- 2020].

AUTHORS

Jonathan Herrera

Was born in Quito, Ecuador in 1994. He did his high school studies in “Unidad Educativa FAE” and is currently obtaining his degree in Engineering in Computer Science in “Escuela Politécnica Nacional”. With a scholarship awarded by the Ecuadorian government as part of the GAR group, he studied 1 year in King’s College London, completing the course of International Science Foundation Programme from September 21 of 2015 to June 10 of 2016. During his years of study, he has obtained first place in numerous contests in the field of mathematics.

Areas of interest: Artificial Intelligence, Business, Mathematics, Data Science, Machine Learning

Miguel Flores

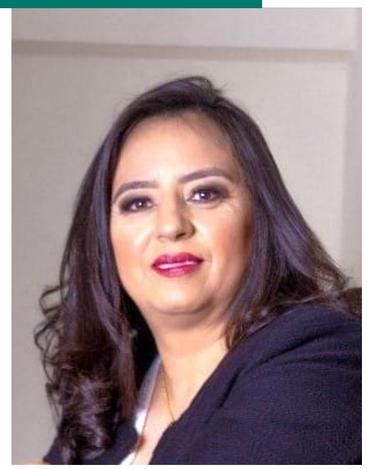
Ph.D. en Estadística e Investigación de Operaciones, Máster en Técnicas Estadísticas (Universidad de La Coruña). Es consultor asociado de LOGIKA Inteligencia de Mercados, consultor asociado en ISVOS que ofrece servicios de investigación estadística en el ámbito económico, social, ambiental y cultural. Es consultor senior asociado en DS ANALYTICS en el área de Big Data y Ciencia de Datos.
Tiene experiencia en Educación y Formación profesional superior, universitaria y empresarial en el campo de la Statistics & Machine Learning aplicado a
los negocios e industrias. Profesor Titular de la cátedra Probabilidad y Estadística, en la Escuela Politécnica Nacional, Departamento de Matemática. Miembro del Grupo de Investigación Multidisciplinar en Sistemas de Información, Gestión de la Tecnología e Innovación (SIGTI) de la Escuela Politécnica Nacional y del Grupo de Modelización, Optimización e Inferencia Estadística (MODES) de la Universidad de La Coruña. Especialista en el desarrollo de metodologías y paquetes estadísticos en R (qcr y ILS)

ISSN: 1390 -9266 – 2020 LAJC

Roberto Omar Andrade

Estudiante de doctorado en Sistemas de Seguridad en la Facultad de Ingeniería de Sistemas en la Escuela Politécnica Nacional (EPN), su maestría es en Gestión de Redes y Telecomunicaciones en la Escuela Politécnica del Ejército en 2013 y su título de ingeniero es en Electrónica y Telecomunicaciones en la Escuela Politécnica Nacional (EPN) en 2007. Oficial de Seguridad del Ministerio de Educación de Ecuador (MINEDUC) en 2015, Coordinador de Infraestructura Tecnológica en la Secretaría Nacional de Planificación SENPLADES 2013-2014, Centro de datos, seguridad y administración de redes en SENPLADES y Tecnología Sucre 2009-2013 e Ingeniería Técnica para sistemas VoIP en SERATVoIP 2007-2011. Es instructor técnico certificado de CCNA, CCNP y CCNA Security en EPN desde 2010 hasta la fecha.

Susana Cadena



Professor at the Universidad Central del Ecuador (UCE), Doctor in Computer Science, in the line of Data Quality and Open Data. Member of the research groups: Indicators for the Management of the Ecuadorian University, State of the IT of the Ecuadorian Universities sponsored by the Ecuadorian Consortium for the Development of Research and Academy (CEDIA) and Group of Analytics and Big Data for the Cybersecurity, in addition to the groups Ecuadorian Network of Open Data and Metadata (REDAM) and Open Science Research Group.

LATIN-AMERICAN JOURNAL OF COMPUTING (LAJC), Vol VII, Issue 2, December 2020

Diseño e implementación de una red inalámbrica de sensores con tecnología LoRa para monitoreo industrial

Design and implementation of a wireless sensor network with LoRa technology for industrial monitoring

ARTICLE HISTORY

Received 01 October 2020
Accepted 16 October 2020

Adrián E. Heredia
Facultad de Ingeniería
Universidad de Cuenca
Cuenca, Ecuador
emilio.heredia@ucuenca.edu.ec

Paúl F. Lucero
Facultad de Ingeniería
Universidad de Cuenca
Cuenca, Ecuador
paul.lucero@ucuenca.edu.ec

Fabián Astudillo Salinas
Facultad de Ingeniería
Universidad de Cuenca
Cuenca, Ecuador
fabian.astudillos@ucuenca.edu.ec

Andrés Vázquez Rodas
Facultad de Ingeniería
Universidad de Cuenca
Cuenca, Ecuador
andres.vazquez@ucuenca.edu.ec

Diseño e implementación de una red inalámbrica de sensores con tecnología LoRa para monitoreo industrial

Design and implementation of wireless sensor network with LoRa technology for industrial monitoring

Adrián E. Heredia
Facultad de Ingeniería
Universidad de Cuenca
Cuenca, Ecuador
emilio.heredia@ucuenca.edu.ec

Paúl F. Lucero
Facultad de Ingeniería
Universidad de Cuenca
Cuenca, Ecuador
paul.lucero@ucuenca.edu.ec

Fabián Astudillo Salinas
Facultad de Ingeniería
Universidad de Cuenca
Cuenca, Ecuador
fabian.astudillos@ucuenca.edu.ec

Andrés Vázquez Rodas
Facultad de Ingeniería
Universidad de Cuenca
Cuenca, Ecuador
andres.vazquez@ucuenca.edu.ec

Abstract — The growing development of the Internet of Things (IoT) has diversified its fields of application, improving not only the interconnection of people but as well the communication between industrial machinery (M2M, Machine-to-Machine), in which its features in range, scalability, and low cost of deployment can be taken advantage of. LoRa and LoRaWAN technologies are presented as one of the main low-cost wireless communication options in the integration of industrial systems with a view to the new requirements of Industry 4.0. In this work, a measurement campaign and the analysis of the data obtained were performed to evaluate the behavior and applicability of LoRa and LoRaWAN technologies within industrial environments. To contrast the results, tests were performed in clear urban environments, where it was observed that the conditions inside the industrial buildings allow the establishment of a link with favorable radio frequency conditions. Initially, short-range scenarios (<100 m) have been considered in which a line of sight is maintained between the transmitter and the receiver.

Keywords — LoRa, LoRaWAN, IoT, Industry 4.0

Resumen — *El creciente desarrollo del Internet de las Cosas (IoT, Internet of Things) ha diversificado sus campos de aplicación, mejorando no solo la interconexión de personas, sino también, la comunicación entre maquinaria industrial (M2M, Machine-to-Machine), en las que sus características en alcance, escalabilidad y bajo costo de despliegue, pueden ser aprovechadas. Las tecnologías LoRa y LoRaWAN se muestran como una de las principales opciones de comunicación inalámbrica de bajo costo en la integración de sistemas industriales con mira a los nuevos requerimientos de la Industria 4.0. En este trabajo se realizó una campaña de mediciones y el análisis de los datos obtenidos, para evaluar el comportamiento y la aplicabilidad de las tecnologías LoRa y LoRaWAN dentro de ambientes industriales. Para contrastar los resultados, se realizaron pruebas en ambientes urbanos despejados, donde se observó que las condiciones dentro de las naves industriales, permiten establecer un enlace con condiciones de radio frecuencia favorables. Inicialmente se han considerado escenarios de corto alcance (<100 m) en los que se mantiene una línea de vista entre el transmisor y el receptor.*

Palabras clave — *LoRa, LoRaWAN, IoT, Industria 4.0.*

ISSN: 1390 -9266 – 2020 LAJC

A. Heredia, P. Lucero, F. Astudillo-Salinas and A. Vázquez-Rodas, “Diseño e implementación de una red inalámbrica de sensores con tecnología LoRa para monitoreo industrial”, Latin-American Journal of Computing (LAJC), vol. 7, no. 2, 2020.

I. INTRODUCCIÓN

En el mercado industrial competitivo, las empresas enfrentan la creciente necesidad de mejorar la eficiencia de sus procesos, ajustarse a regulaciones ambientales y alcanzar metas financieras. Debido a la edad avanzada de muchos de los sistemas industriales y la manufactura dinámica que obliga el mercado, los sistemas de automatización industrial de bajo costo, son una alternativa para optimizar la productividad y eficiencia. Una opción posible es el proponer integraciones al hardware existente (PLCs (Programmable Logic Controller) y Panel HMI (Human-Machine Interface)), sin la necesidad de actualizar equipos o detener el proceso de producción [1],[2]. Tradicionalmente, los sistemas de automatización industrial se realizan por medio de comunicaciones cableadas (Ethernet industrial, RS-232, RS-485). Sin embargo, estos requieren de costosos, invasivos y complejos tendidos, o incluso se requiere adaptar sistemas cuando el hardware es anticuado.

La naturaleza colaborativa y espontánea de las redes inalámbricas de sensores (WSN, Wireless Sensor Network), brinda grandes ventajas sobre los sistemas tradicionales de monitoreo y control cableados, incluyendo auto organización, despliegue rápido, flexibilidad y costo reducido. En este aspecto, las WSN tienen un rol importante para crear sistemas confiables y resistentes que respondan rápidamente a eventos en tiempo real.

En este contexto, los avances actuales en las redes de bajo consumo y largo alcance (LPWAN, Low Power Wide Area Network), y la implementación de sistemas embebidos de automatización y recolección de datos, se han vuelto más factibles para la interconexión de las “islas” de monitoreo industrial [3]. Para aplicaciones industriales existen varias alternativas. En algunas especificaciones como Zigbee y WirelessHART, se usa el estándar IEEE 802.15.4 [4], [5]. En la tecnología LoRa, por su parte, se utiliza mayormente la especificación LoRaWAN, aunque es posible usar también el estándar 802.15.4. La tecnología LoRa fue desarrollada por The LoRa Alliance [6], y ha tenido una mayor aceptación en el mercado en los últimos años por sus características superiores en parámetros como alcance, robustez y bajo consumo de energía [7]. Así, se espera que la tecnología LoRa también se adapte satisfactoriamente a los requerimientos de aplicaciones enfocadas en la Industria 4.0 [8].

Con las LPWAN se abre una perspectiva industrial diferente, gracias al lanzamiento continuo de nuevos equipos. Entre estos se destacan los desarrollados por el fabricante de semiconductores SEMTECH con su línea de productos de largo alcance “Long-Range” (LoRa) [9]. LoRa hace uso de tecnologías avanzadas de espectro ensanchado [10], utilizando pulsos modulados de frecuencias lineales de banda ancha para lograr mejores características de frecuencia [11], [12].

LoRaWAN, por su parte, define el protocolo de comunicación (capa de enlace de datos del modelo OSI) y la arquitectura del sistema, sobre la capa física definida por LoRa [13]. LoRaWAN utiliza una topología en estrella de largo alcance en la que los gateways son usados para conmutar los mensajes entre los dispositivos finales (nodos) y el núcleo de la red [14]. En una red LoRaWAN los nodos pueden transmitir los datos a múltiples gateways y no necesariamente a uno solo. A su vez, cada gateway direccionará los paquetes recibidos desde el nodo final al servidor de red, que puede ser local o que puede estar ubicado en la “nube”. Esto se realiza a través de algún tipo de backhaul, tradicionalmente mediante: GSM, LTE, Ethernet, satélite, o WiFi [15], [16].

Hoy la industria muestra especial interés en la conexión de la parte física (equipos de piso) y la infraestructura digital, con el fin de optimizar la producción y proporcionar interoperabilidad a las diferentes entidades involucradas, satisfaciendo directrices de la Industria 4.0 [17], [18]. Por lo que en este trabajo se propone la evaluación de una red LoRaWAN y su aplicabilidad en entornos industriales. Se realizaron campañas de mediciones, además de pruebas controladas en ambientes libres de obstáculos y fuentes de interferencia. Los datos recopilados muestran que los parámetros de calidad: RSSI (Received Signal Strength Indication), SNR (Signal-to-Noise Ratio) y tasa de pérdida de paquetes, presentan poca degradación causada por los equipos y maquinarias dentro de los ambientes industriales, obteniendo niveles más favorables que en ambientes urbanos despejados. La adquisición de datos se realizó por un proceso de muestreo por cada punto de medición.

El resto del documento está organizado de la siguiente manera. La Sección II analiza los trabajos relacionados. En la Sección III se hace una revisión general de los aspectos más relevantes de la capa física LoRa y el protocolo LoRaWAN. Por su parte, en la Sección IV se presenta la metodología propuesta para la evaluación. La Sección V muestra los resultados obtenidos y finalmente en la Sección VI se presentan las principales conclusiones de este trabajo.

II. TRABAJOS RELACIONADOS

En los últimos años, varios trabajos se han centrado en las tecnologías utilizadas para despliegues de IoT, destacando recientemente LoRa y LoRaWAN. De estas últimas, en varios trabajos, se ha analizado su aplicabilidad y desempeño en ambientes con factores adversos para las transmisiones de radio (interferencia, ruido, reflexión).

Una de las principales deficiencias de las tecnologías de IoT, es proveer datos en tiempo real. En [8] se describen estrategias para optimizar la capa de acceso (MAC), tanto para transmisiones periódicas en tiempo real y transmisiones ocasionales no periódicas. Para esto, se busca sincronizar la transmisión de los nodos finales con el fin de evitar colisiones. Estas optimizaciones permiten seguir explotando las ventajas de las WSN, como la alta escalabilidad y reducida infraestructura, necesaria para su despliegue.

Por su parte, en [6] se evalúa la capacidad de la tecnología LoRa para comunicaciones de largo alcance, siendo posible lograr máximos de hasta 10 kilómetro con condiciones de línea de vista.

El trabajo de [19] muestra cómo las capacidades de largo alcance de LoRa pueden ser aprovechadas en aplicaciones industriales de corto alcance, en las que el principal atenuante es la interferencia producida por los equipos de alta potencia. El desempeño de la tecnología LoRa no es equivalente al de sistemas cableados, pero con una tasa de error de paquetes cercana al 0.2 %, esta se muestra como una solución para sistemas industriales no críticos.

El despliegue de una red LoRaWAN dentro de las instalaciones de un barco militar se expone en [20]. En este caso, las condiciones son adversas debido a la estructura de metal que provoca reflexiones de las señales de radio, además de la ausencia de línea de vista para la transmisión de los nodos sensores. La red logró un desempeño aceptable utilizando un factor de ensanchamiento (SF, Spreading Factor), con valor de 12. Se alcanza una tasa de pérdida de paquetes (PER, packet error ratio) inferior al 5 % en una longitud de 110 m entre compartimientos de la nave. En este estudio, LoRaWAN se presenta como una alternativa al despliegue de cable de cobre o fibra óptica, que en el caso de navíos implica gran complejidad y elevados costos.

LoRaWAN permite que la red sea escalable y facilita la movilidad de los nodos sensores. En [21] se analiza el desempeño de una WSN en el interior de una mina. Se considera que este ambiente sufre cambios constantes en su estructura, además de variaciones en niveles de gases, humedad y temperatura. Por tanto, se requiere un monitoreo continuo, tanto de la maquinaria como de las condiciones ambientales a las que se expone el personal. En dicho trabajo se reduce el retardo y la latencia en la transmisión de paquetes. Se mejora así el desempeño de la red en caso de transmisiones de emergencia, que requieren el menor número de retransmisiones en el caso de pérdida o errores en los paquetes.

Las capacidades de la tecnología LoRa para comunicaciones de largo alcance se ha analizado profundamente en múltiples trabajos, logrando distancias superiores a los 10 km con línea de vista. Para esto, las redes basan su arquitectura en una topología en estrella empleando el protocolo LoRaWAN. Por otro lado, [22] analiza que este tipo de estructura de red es dependiente de la línea de vista entre dispositivos, sin embargo, esto no siempre es posible. Específicamente, el trabajo se enfoca en la detonación de explosivos dentro de minas empleando tecnología LoRa para la transmisión en una red multi-salto, capaz de superar obstáculos en ambientes irregulares.

III. TECNOLOGÍAS LORA Y LORAWAN

A. LoRa

LoRa es un tipo de modulación de capa física de espectro ensanchado CSS (Chirp Spread Spectrum) [23]. Esta modulación consiste en el uso de una señal chirp que varía constantemente con la frecuencia. Esto permite de cierta forma que aumente su capacidad de resistencia a señales interferentes y además reduce el desvanecimiento de la señal debido a la propagación multi-camino [24]. Esto a su vez implica que, los nodos que se encuentren más cercanos al Gateway tendrán una tasa de datos mayor que la de los nodos más alejados [23]. Además, al ser un estándar LPWAN es posible reducir la tasa efectiva de transmisión de datos

ISSN: 1390 -9266 – 2020 LAJC

cuando existan rangos de comunicación más amplios que requieren un enlace más robusto [24].

El bajo consumo energético y su gran alcance, hacen que LoRa sea uno de los estándares más utilizados en el desarrollo de aplicaciones IoT industriales (IIoT). Lo cual permite que los dispositivos usados en este tipo de desarrollos industriales aumenten su tiempo de vida. Sin embargo, en algunos casos LoRa presenta ciertos inconvenientes en cuanto a la latencia. En la actualidad, existen otros protocolos que podrían proporcionar una latencia más baja y una velocidad de datos más alta, por ejemplo NB-IoT (Narrow Band IoT) [25].

Por otra parte, una de las mayores ventajas de LoRa radica en el uso de una amplia gama de frecuencias que no requieren licencia, ya que pertenecen al espectro ISM (Industrial, Scientific and Medical). Esto facilita la interoperabilidad en todo el mundo [23].

B. LoRaWAN

La especificación LoRaWAN es un protocolo de red de bajo consumo y largo alcance, LPWAN [26]. Su funcionamiento se basa en dispositivos de bajo consumo energético usados generalmente en el desarrollo de aplicaciones relacionadas al IoT y al IIoT.

Una red LoRaWAN cuenta con una topología conocida como Estrella de Estrellas (Star of Stars), compuesta por cuatro elementos principales: dispositivos finales, Gateway, un servidor de red y un servidor de aplicación. Los dispositivos finales generalmente se encuentran conformados por sensores o actuadores, los cuales comparten con el gateway la información adquirida, haciendo uso de la capa física LoRa. Por su parte, el gateway se encarga de receptar dicha información y compartirla con el servidor de red mediante una comunicación basada en el protocolo IP [27].

El protocolo LoRaWAN cuenta con características que permiten recopilar datos en un solo Gateway desde varios nodos ubicados a diferentes distancias, incluso kilómetros, mediante una comunicación unidireccional [15]. Sin embargo, en algunos casos se ha optado por la comunicación bidireccional entre nodo y gateway, y existe también la posibilidad de tener más de un gateway.

La función de los gateways radica en el envío de la información recolectada de cada dispositivo final, sin procesar, a un servidor de red mediante un interfaz de backhaul de mayor rendimiento como Ethernet, 3G/4G, satélite o Wi-Fi [28].

Por su parte, el servidor de red recibe la información enviada en forma de paquetes desde los nodos, los decodifica y realiza su protocolo de seguridad. De esta manera, cada una de las aplicaciones que se ejecutan en los servidores de aplicaciones, pueden recibir los datos desde el servidor de red, y pueden usar dicha información a su conveniencia [29].

En la Figura 1 se puede observar cada uno de los componentes de la arquitectura descrita. Esta arquitectura LoRaWAN basada en la topología estrella de estrellas permite garantizar una comunicación eficaz entre todos los dispositivos, además de generar un bajo consumo energético en los dispositivos finales.

IV. MÉTODO

Para el despliegue de la red LoRaWAN diseñada en este trabajo, se utilizaron sistemas de código abierto y equipos de bajo costo, adecuados para las condiciones de los escenarios estudiados. Las campañas de medición se realizaron en dos escenarios industriales y dos entornos controlados, con el fin de contrastar resultados. Los escenarios industriales cuentan

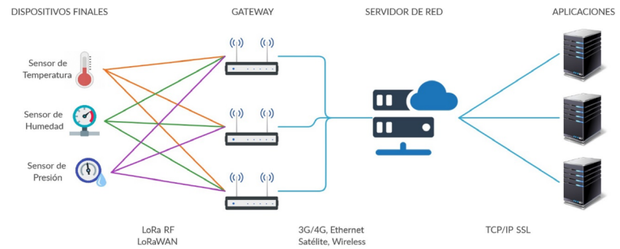


Fig. 1 Arquitectura LoraWAN [30]

con diferentes maquinarias y acometidas ubicadas dentro de naves metálicas, mientras que los escenarios controlados son áreas verdes libres de obstáculos, ubicadas en sectores urbanos.

A. Equipos

1) Heltec WiFi LoRa 32: El equipo Heltec WiFi LoRa 32 es un dispositivo orientado a IoT, diseñado y producido por Heltec Automation. La tarjeta de desarrollo basa su funcionamiento en el microcontrolador ESP32 y se vale del chip integrado SX1278 para las funciones de comunicación LoRa. Estos dos dispositivos interactúan por medio de una interfaz SPI (Serial Peripherical Interface) [31].

A pesar de ser diseñado para operar como nodo sensor, el dispositivo de Heltec puede configurarse también como un gateway LoRaWAN, comunicándose al servidor por medio del protocolo TCP/IP. Esto limita su funcionamiento, impidiéndole realizar transmisiones en el enlace descendente hacia los nodos sensores.

B. Raspberry Pi 3 modelo B

Raspberry Pi 3 es una computadora de dimensiones reducidas, originalmente diseñada con fines educativos por la fundación Raspberry Pi. Puede soportar una variedad de sistemas operativos con un procesador de arquitectura ARM. El ordenador cuenta con periféricos que incluyen pines GPIO (General Purpose Input/ Output), permitiendo la comunicación y control de dispositivos externos [32].

En este trabajo se utilizó la Raspberry Pi 3 modelo B, como administrador de la red LoRaWAN y servidor web, para la conexión con aplicaciones e interfaces gráficas.

C. Disposición de Equipos

En la Figura 2 se muestra la disposición de los equipos en la red LoRaWAN. El nodo sensor está compuesto por un micro-controlador encargado de recopilar mediciones del ambiente, y comunicarlas por un puerto serial hacia el módulo Heltec WiFi LoRa 32 para su transmisión mediante la tecnología LoRa. En el gateway (receptor), se utiliza, al igual que en transmisor, el módulo SX1278 en la tarjeta de Heltec. Los datos recibidos por éste, se transmiten hacia el servidor por medio del módulo WiFi. El servidor está montado sobre la Raspberry Pi, que cumple tanto con las funciones de administrador de la red LoRaWAN como la función de servidor web para el interfaz de usuario.

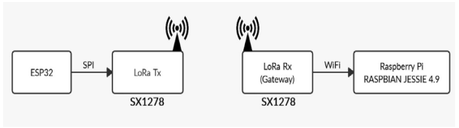


Fig. 2 Diagrama de bloques de los equipos

D. Configuración de Equipos

La configuración de los equipos utilizados en este trabajo se basa en las directrices de The LoRa Alliance [13] para la topología de una red LoRaWAN. En la capa física, se utiliza una frecuencia de 433 MHz, empleando el chip SX1278 de SEMTECH, tanto para el transmisor como para el receptor. El servidor de red se montó sobre un ordenador Raspberry Pi para la administración de la red.

- ***Nodo sensor:*** Los datos a transmitirse desde el nodo sensor son recompilados por medio de una tarjeta Arduino NANO conectada como periférico por medio de un puerto serial al módulo Heltec WiFi LoRa 32. La información de sensores y periféricos es cifrada usando el método Cayenne LPP [33]. Esto con el fin de reducir el tamaño de los mensajes (payload) y enviar varias mediciones por mensaje. El microprocesador ESP32 de la tarjeta Heltec maneja el chip SX1278 y los parámetros de transmisión así como las credenciales de seguridad.

- ***Gateway:*** El chip SX1278 de la tarjeta Heltex WiFi LoRa 32, se encarga de recibir las transmisiones LoRa. Estas son procesadas por el microcontrolador ESP32, que las empaqueta y transmite por la red IP utilizando su módulo WiFi integrado. La programación se basó en el trabajo de [34] para un gateway de canal sencillo.

- ***Servidor:*** El servidor LoRaWAN se monta sobre un ordenador Raspberry Pi 3 modelo B. También se configuró un servidor MQTT para la comunicación con aplicaciones externas y un servidor web para el interfaz de usuario. El servidor y el gateway se comunican por una red WiFi. Los datos procesados por el servidor son almacenados en una base de datos en formato .csv.

ISSN: 1390 -9266 – 2020 LAJC

E. Escenarios

El aporte de este trabajo se centra en evaluar el comportamiento y la aplicabilidad de la tecnología LoRa en ambientes industriales por lo que se eligieron dos instalaciones con diferente maquinaria y procesos de producción. Las mediciones se desarrollaron manteniendo una línea de vista entre el nodo sensor y el gateway. Adicionalmente, se realizaron pruebas controladas en dos ambientes libres de obstáculos y fuentes de interferencia.

a) Ambiente industrial 1: La nave principal del ambiente industrial 1 cuenta con una altura aproximada de 20 m, una longitud superior a los 150 m y se compone de dos niveles. En la planta baja se ubican, en su mayoría, motores de alta potencia (50-120HP). Además, esta superficie funciona como área de almacenaje y preparación de producto terminado. En la planta alta se tienen dos líneas de producción extendidas a lo largo de la nave. Ambas plantas se encuentran divididas por un pasillo central que comunica los ambientes y permite el acceso a la maquinaria.

Para el primer grupo de pruebas en la planta alta, el *gateway* fue colocado en el extremo sur del pasillo, mostrado en la Figura 3, con una altura de 1.5 m con respecto al suelo, mientras que el nodo sensor fue ubicado a diferentes distancias a lo largo del pasillo (Figura 3).

En la segunda planta de la nave principal, se colocó el *gateway* en el extremo sur a una altura de 1.5 m con respecto al suelo, y el nodo fue colocado alejándolo una distancia de 90 m del *gateway*.

En las mediciones en la planta alta y baja, se mantuvo una línea de vista entre el nodo sensor y el gateway. En las áreas de medición, se observó un reducido tránsito de personas y maquinaria pesada (montacargas). Es importante mencionar que debido a las restricciones de seguridad, no fue posible realizar mediciones dentro de los límites de las líneas de producción.

b) Ambiente industrial 2: La fábrica del ambiente industrial 2 se compone de una nave principal dividida en dos alas (Figura 4). Cada una de estas cuenta con una longitud superior a 100 m y una altura aproximada de 20 m. La fábrica se compone de varias líneas de producción, en las que cada etapa del proceso, se cuenta con una maquinaria diferente, teniendo como principales actuadores a motores de alta potencia (50-120HP).

El *gateway* fue ubicado en la segunda planta de las oficinas del área técnica a una altura de cuatro metros con respecto al suelo. Desde este punto se logró mantener una línea de vista hacia las ubicaciones de los nodos sensores.

El primer grupo de pruebas se realizó en el ala norte, colocando el nodo sensor a una altura de 1.5 m sobre el suelo. En esta parte de la fábrica se tiene un tráfico moderado de personal y montacargas, mientras que existe una gran cantidad de maquinaria para producción y empaquetado. El segundo grupo de pruebas se las realizó en el ala sur, ubicando el nodo sensor en el extremo este de la nave, y manteniendo la posición del *gateway* como en las mediciones previas. En esta parte de la fábrica, la maquinaria de producción tiene alturas variables, alcanzando hasta 10 m de altura. En el ala sur, el tránsito de personal y maquinaria es reducido.

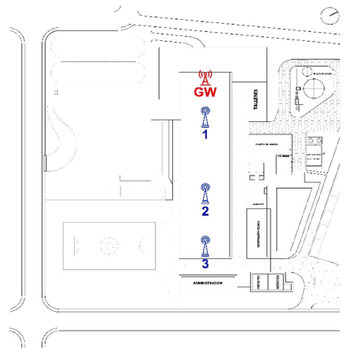


Fig. 3 Distribución del ambiente industrial 1

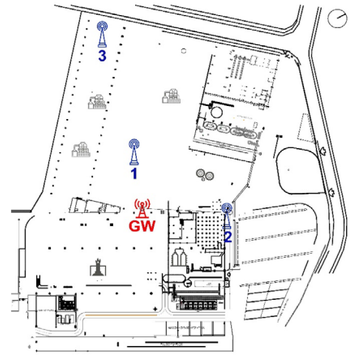


Fig. 4 Distribución del ambiente industrial 2

c) Ambiente urbano abierto 1: Las pruebas de control se realizaron con el fin de contrastarlas con mediciones en ambientes industriales, y evaluar sus variaciones. Se eligió el área del ambiente urbano 1, indicada en la Figura 5. Ésta presenta una extensión en un parque, sin obstáculos y un reducido gradiente, permitiendo mantener una línea de vista desde el nodo sensor hasta el gateway.

El *gateway* fue colocado a una altura de tres metros y el nodo sensor se ubicó a diferentes distancias como se muestra en la Figura 5. En las cercanías del parque no existen fuentes de interferencias visibles (maquinaria, torres celulares, antenas HF). El tráfico de peatones fue reducido durante el periodo de las pruebas.

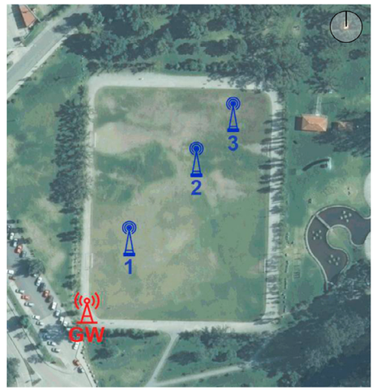


Fig. 5 Ambiente Urbano Abierto 1

d) Ambiente urbano abierto 2: La segunda prueba de control se realizó en otro parque, ubicado en una área urbana al sureste de la ciudad de Cuenca. El parque cuenta con una longitud aproximada de 130 m y un gradiente reducido por lo que permite mantener una línea de vista entre el gateway y el nodo sensor.

El *gateway* fue colocado en el extremo sur del parque a una altura de 3 m. El nodo fue colocado a diferentes distancias a una altura de 1.5 m (Figura 6). En las cercanías del predio no se presentaron fuentes de interferencia. El tráfico de peatones y vehículos en la zona fue moderado.

F. Procedimientos

Los procesos de medición, consistieron en el envío de paquetes desde el nodo sensor (transmisor), manteniendo un factor de ensanchamiento, SF de 7, y una frecuencia de transmisión constante de 433.175 MHz. Se utilizó un valor de potencia de 16 dB, el máximo permitido por el chip. El equipo transmisor se colocó a una altura de 1.5 m sobre el nivel del suelo. El gateway fue colocado a diferentes alturas para lograr mantener una línea de vista con el nodo sensor, esto en función de las condiciones de los ambientes, como se indica en la Sección IV-E.

En cada punto se transmitieron 100 paquetes, de los cuales se recolectó el RSSI, el SNR y el número de paquete para determinar porcentaje de pérdidas. Por las limitaciones de los equipos empleados no se pudo variar el SF, así como tampoco se pudieron aplicar saltos de frecuencia, debido a que esto no es soportado por el chip del receptor (SX1278) [35].

El transmisor y receptor fueron equipados con una antena de 1 dBi de ganancia y alimentados por medio de baterías de litio conectadas a los respectivos conectores micro-USB.

Las fábricas en las que se realizaron las mediciones en ambientes industriales limitaron el acceso a las instalaciones, debido a estrictas medidas de seguridad. Esto redujo la cantidad de mediciones y los puntos a analizar.

Fig. 6 Ambiente Urbano Abierto 2

ISSN: 1390 -9266 – 2020 LAJC

V. RESULTADOS

La red inalámbrica de sensores empleando la capa física LoRa y la arquitectura LoRaWAN se evaluó en dos ambientes industriales con diferentes instalaciones y distribución de equipos. Así también se realizaron mediciones en dos ambientes de control, en los que no existen obstáculos ni fuentes de interferencia cercanas. Debido a que este es un trabajo en curso, los resultados preliminares de las primeras campañas de medición se presentan a continuación.

Los resultados de SNR (Figura 7) y RSSI (Figura 8) recopilados por el servidor LoRaWAN, muestran niveles similares para los dos ambientes industriales. Esto a pesar de las diferencias entre su maquinaria y la disposición de su infraestructura. Los valores de SNR y RSSI son similares a los medidos por [36] en ambientes urbanos y por [37] en ambientes forestales. En estos casos, los niveles para una distancia aproximada de 100 m bordean un SNR cercano a 10 unidades y el RSSI niveles cercanos a 80 dBm. Los valores de SNR y RSSI permitieron un enlace estable en el que el porcentaje de pérdidas de paquetes se mantuvo por debajo del 6 % para todos los casos (Figura 9).

En las mediciones para los escenarios de control se utilizaron parámetros iguales de configuración tanto en el nodo sensor como en el gateway. Los valores de SNR obtenidos en las mediciones de control, muestran niveles de ruido superiores a los obtenidos en ambientes industriales (Figura 7). Las mediciones de RSSI indican una mayor atenuación en todas las distancias analizadas, esto en comparación con los valores obtenidos dentro de las fábricas.

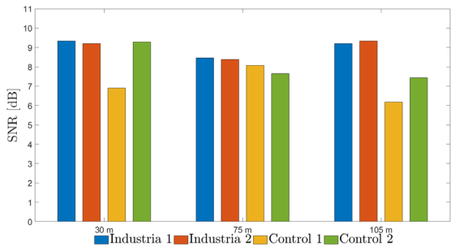


Fig. 7 Resultados de SNR para los ambientes industriales y de control

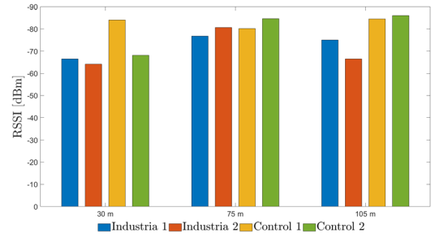


Fig. 8 Resultados de RSSI para los ambientes industriales y de control

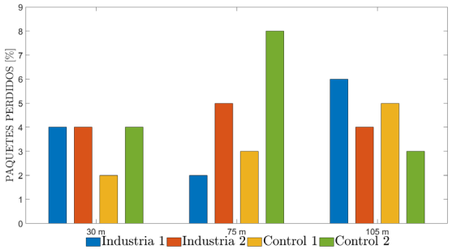


Fig. 9 Resultado de la Tasa de Pérdida de Paquetes

A pesar de las condiciones obtenidas en los ambientes de urbanos abiertos, fue posible establecer un enlace estable con pérdidas de paquetes inferiores al 6 % en la mayoría de los casos.

Los niveles de SNR medidos en los ambientes industriales y urbanos abiertos, indican un posible solapamiento de la señal debido a la propagación multi-camino [38], [39]. En los ambientes industriales, este solapamiento parece afectar de forma constructiva a la señal recibida, debido a las dimensiones y materiales de las naves industriales donde se realizaron las pruebas. En el caso de los parques de los escenarios urbanos abiertos, se observa un solapamiento con efectos de cancelación, provocando los bajos niveles de SNR medidos. El parque elegido como segundo escenario urbano abierto, mostró mejores niveles de SNR y RSSI, en contraste con el primer escenario de control. El segundo parque contaba con una menor área despejada, al estar rodeado por una zona urbana residencial. Estas condiciones afectaron en menor manera el desface y retardo de la señal. Por las limitaciones de los equipos empleados, se utilizó solo un SF de 7, según [39] esta configuración permite una gran sensibilidad a los efectos de la propagación multi-camino en un canal Rayleight [40].

VI. CONCLUSIONES

Los primeros resultados presentados en este trabajo muestran una importante evidencia de la aplicabilidad de la tecnología LoRa y la arquitectura LoRaWAN, en comunicaciones de corto alcance para ambientes industriales. La WSN provee una robustez y escalabilidad adecuada para el monitoreo de eventos recurrentes y aleatorios que influyen en procesos de producción y mantenimiento.

El reducido costo, baja complejidad y seguridad de los nodos sensores y gateways, facilitan su despliegue e inter- operabilidad, sin necesidad de una infraestructura existente.

Las fuentes de ruido e interferencia (motores trifásicos AC, acometidas de alta tensión, estructuras metálicas, redes WAN) identificadas en los ambientes de pruebas, no influyeron de forma considerable en la calidad del enlace, a pesar de que tanto el nodo sensor como el gateway se ubicaron en alturas cercanas al nivel del suelo.

Los parámetros de SNR, RSSI y PER, muestran poca degradación en la calidad del enlace dentro de los ambientes industriales analizados. En contraste, en las pruebas de control, se observó que los ambientes urbanos abiertos 1 y 2, cuentan con niveles considerablemente superiores de SNR, y valores similares de RSSI y PER. Esto lleva a intuir que la nave metálica de las fábricas atenúa interferencia y ruido del exterior, además de reducir efectos destructivos de la propagación multi-camino, a la cual es más sensible el enlace configurado con un SF de 7.

El chip SX1278 cumplió satisfactoriamente las funciones de transmisor en el nodo sensor. Al ser configurado como gateway, la fiabilidad del chip de la tarjeta Heltec WiFi LoRa, puede disminuir, debido a que no está diseñado para cumplir con estas funciones.

En trabajos futuros se complementarán las campañas iniciales de medición, analizando con mayor detalle los escenarios de control y la cantidad de paquetes y repeticiones por medición. Se ve oportuno además el análisis de los efectos de dispersión multi-camino dentro de naves y estructuras metálicas así como en ambientes urbanos, en especial para SF superiores al analizado en este trabajo. Otro aspecto, sería evaluar la ubicación de gateways en niveles más elevados de las naves industriales, que faciliten una línea de vista desde cualquier punto de las instalaciones. Este trabajo también es un primer paso para evaluar la factibilidad de implementar soluciones industriales concretas basadas en la tecnología LoRa en las industrias locales.

VII. REFERENCIAS

[1] V. Gungor and G. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," IEEE Transactions on Industrial Electronics, vol. 56, no. 10, pp. 4258–4265, Oct. 2009. [Online]. Available: http://ieeexplore.ieee.org/document/4796311/ [Accessed: Oct.22, 2020].

[2] L. Li, J. Ren, and Q. Zhu, "On the application of LoRa LPWAN technology in Sailing Monitoring System," in 2017 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS). Jackson, WY, USA: IEEE, Feb. 2017, pp. 77–80. [Online]. Available: http://ieeexplore.ieee.org/document/7888762/ [Accessed: Oct.22, 2020].

[3] I. F. Akyildiz and M. C. Vuran, Wireless sensor networks, ser. Ian F. Akyildiz series in communications and networking. Chichester, West Sussex, U.K. ; Hoboken, NJ: Wiley, 2010, oCLC: ocn564132645.

[4] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of WirelessHART and ZigBee for industrial applications," in 2008 IEEE International Workshop on Factory Communication Systems. Dresden, Germany: IEEE, May 2008, pp. 85–88. [Online]. Available: http://ieeexplore.ieee.org/document/4638746/ [Accessed: Oct.22, 2020].

[5] S. Lin, J. Liu, and Y. Fang, "ZigBee Based Wireless Sensor Networks and Its Applications in Industrial," in 2007 IEEE International Conference on Automation and Logistics. Jinan, China: IEEE, Aug. 2007, pp. 1979–1983. [Online]. Available: http://ieeexplore.ieee.org/document/4338898/ [Accessed: Oct.22, 2020].

[6] S. Devalal and A. Karthikeyan, "LoRa Technology - An Overview," in 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). Coimbatore: IEEE, Mar. 2018, pp. 284–290. [Online]. Available: https://ieeexplore.ieee.org/document/8474715/ [Accessed: Oct.22, 2020].

[7] M. Rizzi, P. Ferrari, A. Flammini, E. Sisinni, and M. Gidlund, "Using LoRa for industrial wireless networks," in 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). Trondheim, Norway: IEEE, May 2017, pp. 1–4. [Online]. Available: http://ieeexplore.ieee.org/document/7991972/ [Accessed: Oct.22, 2020].

[8] L. Leonardi, F. Battaglia, G. Patti, and L. L. Bello, "Industrial LoRa: A Novel Medium Access Strategy for LoRa in Industry 4.0 Applications," in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society. Washington, DC: IEEE, Oct. 2018, pp. 4141–4146. [Online]. Available: https://ieeexplore.ieee.org/document/8591568/ [Accessed: Oct.22, 2020].

[9] V. J. Hodge, S. O'Keefe, M. Weeks, and A. Moulds, "Wireless Sensor Networks for Condition Monitoring in the Railway Industry: A Survey," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 3, pp. 1088–1106, Jun. 2015. [Online]. Available: http://ieeexplore.ieee.org/document/6963375/ [Accessed: Oct.22, 2020].

[10] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855–873, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7815384/ [Accessed: Oct.22, 2020].

[11] M. Aref and A. Sikora, "Free space range measurements with semtech lora™ technology," in 2014 2nd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems, 2014, pp. 19–23.

[12] S. Daud, T. S. Yang, M. A. Romli, Z. A. Ahmad, N. Mahrom, and R. A. A. Raof, "Performance Evaluation of Low Cost LoRa Modules in IoT Applications," IOP Conference Series: Materials Science and Engineering, vol. 318, p. 012053, Mar. 2018. [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/318/1/012053 [Accessed: Oct.22, 2020].

[13] LoRa-Alliance, "About LoRaWAN® | LoRa Alliance®," 2020. [Online]. Available: https://lora-alliance.org/about-lorawan [Accessed: Oct.22, 2020].

[14] R. F. A. M. Nor, F. H. K. Zaman, and S. Mubdi, "Smart traffic light for congestion monitoring using LoRaWAN," in 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC). SHAH ALAM, Malaysia: IEEE, Aug. 2017, pp. 132–137. [Online]. Available: http://ieeexplore.ieee.org/document/8070582/ [Accessed: Oct.22, 2020].

[15] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia- Segui, and T. Watteyne, "Understanding the Limits of LoRaWAN," IEEE Communications Magazine, vol. 55, no. 9, pp. 34–40, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8030482/

[16] L. Casals, B. Mir, R. Vidal, and C. Gomez, "Modeling the Energy Performance of LoRaWAN," Sensors, vol. 17, no. 10, p. 2364, Oct. 2017. [Online]. Available: http://www.mdpi.com/1424-8220/17/10/2364 [Accessed: Oct.22, 2020].

[17] S.-I. Toc and A. Korodi, "Modbus-OPC UA Wrapper Using Node-RED and IoT-2040 with Application in the Water Industry," in 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY). Subotica: IEEE, Sep. 2018, pp. 000 099–000 104. [Online]. Available: https://ieeexplore.ieee.org/document/8524749/ [Accessed: Oct.22, 2020].

[18] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which Wireless Technology for Industrial Wireless Sensor Networks? The Development of OCARI Technology," IEEE Transactions on Industrial Electronics, vol. 56, no. 10, pp. 4266–4278, Oct. 2009. [Online]. Available: http://ieeexplore.ieee.org/document/5173521/ [Accessed: Oct.22, 2020].

[19] L. Tessaro, C. Raffaldi, M. Rossi, and D. Brunelli, "LoRa Performance in Short Range Industrial Applications," in 2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM). Amalfi: IEEE, Jun. 2018, pp. 1089–1094. [Online]. Available: https://ieeexplore.ieee.org/document/8445392/ [Accessed: Oct.22, 2020].

ISSN: 1390 -9266 – 2020 LAJC

[20] F. Gui, Y. Yin, and A. Lu, “Research on ship wireless communication technology based on lora,” in 2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Confe- rence (IMCEC), 2018, pp. 976–979.
[21] A. Nessa, F. Hussain, and X. Fernando, “Adaptive latency reduction in lora for mission critical communications in mines,” in 2020 IEEE Conference on Communications and Network Security (CNS), 2020, pp. 1–7.
[22] P. Branch and T. Cricenti, “A lora relay based system for detonating ex- plosives in underground mines,” in 2020 IEEE International Conference on Industrial Technology (ICIT), 2020, pp. 259–264.
[23] M. O. Farooq and D. Pesch, “Analyzing lora: A use case perspective,” in 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE, 2018, pp. 355–360.
[24] A. Lavric and V. Popa, “Internet of things and lora™ low-power wide- area networks: a survey,” in 2017 International Symposium on Signals, Circuits and Systems (ISSCS). IEEE, 2017, pp. 1–5.
[25] R. S. Sinha, Y. Wei, and S.-H. Hwang, “A survey on lpwa technology: Lora and nb-iot,” Ict Express, vol. 3, no. 1, pp. 14–21, 2017.
[26] T. Bouguera, J.-F. Diouris, J.-J. Chaillout, R. Jaouadi, and G. Andrieux, “Energy consumption model for sensor nodes based on lora and lora- wan,” Sensors, vol. 18, no. 7, p. 2104, 2018.
[27] L. Casals, B. Mir, R. Vidal, and C. Gomez, “Modeling the energy performance of lorawan,” Sensors, vol. 17, no. 10, p. 2364, 2017.
[28] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, “A study of lora: Long range & low power networks for the internet of things,” Sensors, vol. 16, no. 9, p. 1466, 2016.
[29] J. de Carvalho Silva, J. J. Rodrigues, A. M. Alberti, P. Solic, and A. L. Aquino, “Lorawan—a low power wan protocol for internet of things: A review and opportunities,” in 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech). IEEE, 2017, pp. 1–6.
[30] P. San Cheong, J. Bergs, C. Hawinkel, and J. Famaey, “Comparison of lorawan classes and their power consumption,” in 2017 IEEE symposium on communications and vehicular technology (SCVT). IEEE, 2017, pp. 1–6.
[31] H. Automation, “WIFI LoRa 32 (V2).” [Online]. Available: https://heltec.org/project/wifi-lora-32/ [Accessed: Oct.22, 2020].
[32] F. R. Pi, “Raspberry Pi 3 Model B – Raspberry Pi.” [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b/ [Accessed: Oct.22, 2020].
[33] “Cayenne Docs.” [Online]. Available: https://developers.mydevices.com/cayenne/docs/lora/lora-cayenne-low-power-payload
[34] V. Cola, “vpcola/ESP32SingleChannelGateway,” Sep.2020, original-date: 2018-03-03T06:38:08Z. [Online]. Available: https://github.com/vpcola/ESP32SingleChannelGateway [Accessed: Oct.22, 2020].
[35] “SX1278 | 137MHz to 525MHz Long Range Low Power Transceiver | Semtech.” [Online]. Available: https://www.semtech.com/products/wireless-rf/lora transceivers/sx1278 [Accessed: Oct.22, 2020].
[36] C. L. Carrión, “Evaluación del rango de transmisión de LoRa para redes de sensores inalámbricos con LoRaWAN en ambientes urbanos,” Tesis de grado, Universidad de Cuenca, Cuenca, Ecuador, 2018. [Accessed: Oct.22, 2020].
[37] P. Avila, “Evaluación del Rango de Transmisión de LoRa para Redes de Sensores Inalámbricas con LoRaWAN en Ambientes Forestales,” Tesis de grado, Universidad de Cuenca, Cuenca, Ecuador, 2017. [Accessed: Oct.22, 2020].
[38] Y. Ai, M. Cheffena, and Q. Li, “Radio frequency measurements and capacity analysis for industrial indoor environments,” in 2015 9th European Conference on Antennas and Propagation (EuCAP), 2015, pp. 1–5. [Accessed: Oct.22, 2020].
[39] K. Staniec and M. Kowal, “LoRa Performance under Variable Interference and Heavy-Multipath Conditions,” Wireless Communications and Mobile Computing, vol. 2018, Article ID 6931083, Apr. 2018. [Online]. Available: https://doi.org/10.1155/2018/6931083
[40] B. Sklar, “Rayleigh fading channels in mobile digital communication systems. i. characterization,” IEEE Communications magazine, vol. 35, no. 7, pp. 90–100, 1997.

ISSN: 1390 -9266 – 2020 LAJC

A. Heredia, P. Lucero, F. Astudillo-Salinas and A. Vázquez-Rodas, “Diseño e implementación de una red inalámbrica de sensores con tecnología LoRa para monitoreo industrial”, Latin-American Journal of Computing (LAJC), vol. 7, no. 2, 2020.

AUTHORS

Adrián E. Heredia

Recibió el título de tercer nivel en Ingeniería Electrónica y Telecomunicaciones de la Universidad de Cuenca, Cuenca, Ecuador en 2020. Participó en el programa internacional "Seeds for the Future" de Huawei Technologies, Shenzhen, China en 2018 Sus intereses de investigación incluyen redes móviles, redes de sensores inalámbricos y ciberseguridad

Paúl F. Lucero

Recibió el título de tercer nivel en Ingeniería Electrónica y Telecomunicaciones de la Universidad de Cuenca, Cuenca, Ecuador en 2020. Sus intereses de investigación incluyen redes móviles, redes de sensores inalámbricos, redes industriales, sistemas de transmisión por fibra óptica, microondas, enlaces satelitales, automatización, ciberseguridad, cloud computing y Tecnologías de la información.

Fabián Astudillo Salinas

Recibió el título de tercer nivel en Ingeniería de Sistemas de la Universidad de Cuenca, Cuenca, Ecuador, en 2007, y los grados de MSc. y Ph.D del "Institut National Polytechnique de Toulouse", Toulouse, Francia, en 2009 y 2013, respectivamente. Desde 2013 es Investigador a Tiempo Completo del Departamento de Ingeniería Eléctrica, Electrónica y Telecomunicaciones de la Universidad de Cuenca, Cuenca, Ecuador. Sus intereses de investigación incluyen redes de sensores inalámbricos, redes vehiculares, simulación de redes, ciberseguridad y HPC.

Andrés Vázquez Rodas

Recibió el grado de Ingeniero Electrónico en el año 2004 de la Universidad Politécnica Salesiana Cuenca – Ecuador, el grado de Master en Telemática (con honores) de la Universidad de Cuenca – Ecuador in 2010, y el grado de Ph.D. del Departamento de Ingeniería Telemática de la Universitat Politècnica de Catalunya BarcelonaTech (UPC), España en 2015. Desde el 2015, es profesor a tiempo completo en la Universidad de Cuenca en el Departamento de Eléctrica, Electrónica y Telecomunicaciones (DEET). Sus intereses de investigación incluyen redes inalámbricas malladas, redes inalámbricas de sensores, redes industriales y sistemas complejos.

ISSN: 1390 -9266 – 2020 LAJC

A comparative evaluation of the performance of open-source SDN controllers

Evaluación comparativa del rendimiento de controladores SDN de código abierto

ARTICLE HISTORY

Received 01 October 2020
Accepted 16 October 2020

Daniel Haro Mendoza
Facultad de Ingeniería
Universidad Nacional de Chimborazo
Riobamba, Ecuador
dharo@unach.edu.ec

Luis Tello Oquendo
Facultad de Ingeniería
Universidad Nacional de Chimborazo
Riobamba, Ecuador
ltello@unach.edu.ec

Luis A. Marrone
LINTI
Universidad Nacional de La Plata
La Plata, Argentina
lmarrone@linti.unlp.edu.ar

A comparative evaluation of the performance of open-source SDN controllers

Evaluación comparativa del rendimiento de controladores SDN de código abierto

Daniel Haro Mendoza
Facultad de Ingeniería
Universidad Nacional de Chimborazo
Riobamba, Ecuador
dharo@unach.edu.ec

Luis Tello Oquendo
Facultad de Ingeniería
Universidad Nacional de Chimborazo
Riobamba, Ecuador
luis.tello@unach.edu.ec

Luis A. Marrone
LINTI
Universidad Nacional de La Plata
La Plata, Argentina
lmarrone@linti.unlp.edu.ar

Abstract — Software-defined Networking (SDN) constitutes a new era in the development of internetworking. The SDN paradigm splits the data plane from the control plane. It uses controller equipment, which is responsible for centrally managing several network devices simultaneously. This study analyzes three open-source controllers for SDN based on the OpenFlow protocol. Specifically, the performance of FloodLight, OpenDayLight (ODL), and Ryu controllers is evaluated in terms of latency, throughput, and scalability. In doing so, the Cbench tool is used in an emulated environment with Mininet. The results show that the Ryu controller presents the lowest performance in all the evaluated parameters; ODL provides lower latency and FloodLight higher throughput. Regarding scalability, we conclude that Floodlight can be used in small networks, whereas ODL can be used in dense networks. Furthermore, we evaluate their main characteristics, which must be considered for their choice prior to implementation and deployment.

Index Terms — SDN, controller, networking, performance.

Resumen — *Las redes definidas por software (SDN) constituyen una nueva era en el diseño de la interconexión de redes. El paradigma SDN separa el plano de datos del plano de control. Para esto utiliza un equipo controlador, que se encarga de gestionar de forma centralizada varios dispositivos de red al mismo tiempo. Este estudio analiza tres controladores SDN de código abierto basados en el protocol OpenFlow. Específicamente, el rendimiento de los controladores FloodLight, OpenDayLight (ODL) y Ryu son evaluados en términos de latencia, throughput y escalabilidad. Para ello se utilizó la herramienta Cbench en un entorno emulado con Mininet. Los resultados muestran que el controlador presenta un menor rendimiento en todos los parámetros evaluados; ODL tiene una menor latencia y Floodlight un mayor throughput. En lo que tiene que ver a escalabilidad, se concluye que Floodlight es recomendable para redes pequeñas y ODL para redes densas. Además, evaluamos sus principales características, las cuales deben ser tomadas en cuenta para su elección antes de su implementación y despliegue.*

Palabras clave — *SDN, controlador, redes, rendimiento.*

ISSN: 1390 -9266 – 2020 LAJC

I. INTRODUCTION

For a long time, network technologies have evolved slower than other communication technologies [1]. This is mainly because manufacturers design their control logic in network equipment closely, making collaborative work and innovation impossible. The popularization of smart devices, virtualization, cloud computing, and data analytics are some of the innovations that have introduced multiple services and applications. They have diverse performance requirements, such as quality of service (QoS), security, mobility, and scalability. These required performance levels have forced data networks to evolve their traditional technologies. This is how the concept of softwarizing data networks appears to adapt the operation of equipment to the logic of the applications and business objectives. In this context, gaining great popularity, the SDN paradigm appears as an approach to promote innovation in the network through greater flexibility, programming capacity, management, and profitability [2].

The SDN principle is to centralize network intelligence by physically separating the control plane from the data plane through application programming. This intelligence is logically located in controllers that maintain a vision, global management, and communication with network devices through a protocol such as OpenFlow. The paradigm of traditional networks is changing rapidly with the advent of SDN; companies that process large amounts of data, such as Facebook and Google [3], are migrating their networks towards software-defined approaches.

The popularization of SDNs has led to many controllers' appearance-based mainly on the OpenFlow protocol; therefore, choosing the right controller for implementation becomes a primary task for the network operator. Moreover, the analysis of parameters and selection criteria constitutes a research opportunity. These drivers were developed by universities, device manufacturers, or research groups, written in different programming languages for multiple applications, and used various techniques to improve their performance.

A comparative study of a controller's main operating parameters in a software-defined network with open source tools is presented in this work. For this, the three controllers that are among the most widespread and implemented have been chosen, namely OpenDaylight (ODL), Ryu, and Floodlight. Additionally, tools for their evaluation, challenges, and research opportunities that can be exploited in future work on this topic are reviewed.

The remainder of this article is structured as follows. Section II reviews the related work on the comparison of SDN controllers. Section III presents a theoretical foundation, background information on software-defined networks, and relevant works related to a controller's role within the SDN network. Section IV presents the network scenario and the software used to evaluate the controllers chosen for the study; a summary of the essential characteristics and functions of the tools used is also presented. Section V presents the evaluations carried out in each of the controllers in terms of latency, throughput, and scalability. Finally, conclusions and future challenges are described in Section VI and VII, respectively.

II. RELATED WORK

Concerning the comparison of SDN controllers, studies such as [4] have been carried out where the ability to handle high traffic loads by SDN controllers is evaluated, carrying out Denial of Service (DoS) attacks on the underlying hosts of the net. It is concluded that the ONOS and ODL drivers are the ones that achieve the best performance. This study uses Mininet with a linear topology with three hosts, while JMeter is used as a tool for load and stress tests in the communication between the controller and the SDN applications.

In [5], the performance of SDN controllers such as Beacon, Pox, Floodlight, and Ryu is compared considering latency and throughput depending on the network's size, up to 100 switches. For the evaluation, the Cbench tool is used in an Ubuntu virtual machine. The results show that Floodlight has a lower latency as the number of Switches in the network increases; in terms of performance, the best performers are Floodlight and Beacon, with almost identical behavior.

In [6], the Cbench tool is used to evaluate the ONOS, Ryu, Floodlight, and OpenDayLight drivers' throughput and latency. In this study, a comparison of each controller's essential operating characteristics is made first,

recommending OpenDayLight for its support. Regarding the performance evaluation, ONOS is recommended, while Ryu presented the best results in latency. One of the limitations of this study is that the comparison is made for network environments with up to 32 switches; that is, the performance in large networks is not evaluated. Another study [7] compares the Floodlight and Ryu controllers' performance in terms of latency and throughput using Mininet and the qperf performance measurement tool. The comparison of the two controllers is made through different experiments on different SDN network topologies. The results show that Floodlight performs better than Ryu, transmitting higher bandwidth and lower latency in all deployed topologies.

In [8], 12 widely used controllers are qualitatively and quantitatively evaluated. In addition to the performance analysis and support criteria, a performance test in terms of latency, throughput, and threads is carried out with the Cbench tool on Ubuntu 14.04. The results describe better performance in C and Java-based drivers, while Python-based drivers such as POX did not show efficient performance. It is also concluded that the best controller's choice to implement will depend on the requirements and its application.

In general, the related works focus on performance evaluation in terms of latency and throughput. We can also realize that the most efficient, used, and recommended controllers are Floodlight, ODL, and Ryu, limiting our study for these three controllers. One of the study's contributions is the scalability evaluation that has not been deepened in previous studies. With the help of the latency and throughput parameters, we will know what the network's performance is in saturated or large-scale scenarios so that the reader can decide which controller to use for different sizes of the network. For this, in the test scenarios, the number of switches increases, reaching up to 256 with 10,000 hosts. Like other studies, we used the Mininet tool to emulate different SDN and Cbench topologies for performance testing.

III. BACKGROUND INFORMATION

Considering scenarios with multiple operators, applications, networks sharing the same infrastructure, services with very different QoS requirements, and a highly dynamic and changing environment, using traditional interconnectivity and network management techniques are not the best option [9]. This is mainly due to the following reasons:

- It is almost impossible to find an optimal performance by configuring quality of service and prioritization techniques for traffic, users, and applications in environments as complex as those mentioned above.

- The dynamism of these networks makes it difficult for them to operate in a stationary regime, introducing complexity to add or remove devices, difficulty applying policies, dependence on suppliers, and inability to respond to changing business needs.

Then, SDN is presented as a new concept to meet new needs. It aims to transform the architectures and management of networks, as is known today [2].

A. SDN Architecture

SDN has become a popular concept, so there is no universal vision of it, as it still depends on the manufacturer that implements it in its infrastructure [10].

There is a variety of definitions for SDN. However, the one made by the Open Networking Foundation (ONF) in [11] can be cited, which is widely accepted: "Software-defined networks are defined as dynamic, manageable network architecture, adaptable, cost-efficient, which makes it ideal for the high bandwidth demands and dynamic nature of today's applications. This architecture decouples the control of the network and the functionality of forwarding of information, allowing that the control of the network can be completely programmable, achieving that the applications and network services are abstracted from the underlying network infrastructure."

The network devices' control function is eliminated and transferred to the controller by separating the control and data planes, as illustrated in Fig. 1.

ISSN: 1390 -9266 – 2020 LAJC

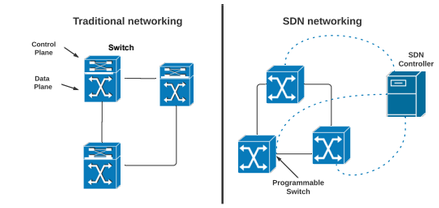


Fig. 1. SDN basic diagram.

The ONF is a non-profit consortium made up of institutions and companies in the IT area dedicated to developing, standardization, and commercializing SDNs. Fig. 2 illustrates the three-layer architecture proposed by the ONF. The devices only care about the forwarding of packets in the infrastructure layer, based on the rules defined by one or more SDN controllers of the control layer, according to the programming logic required and predefined in the application layer [12].

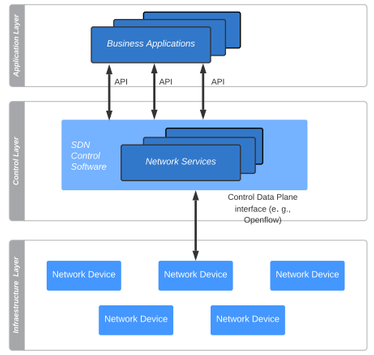


Fig. 2. SDN architecture.

According to ONF [13], the key aspects that characterize the implementation of an SDN architecture are programmability, logically centralized architecture, abstraction, independence, and the use of open standard, as described in Table I.

TABLE I. CHARACTERISTICS OF AN SDN ARCHITECTURE

Characteristic	Description
Programmability	Because forwarding functions were decoupled, it allows that the applications interact with the network.
Logically centralized intelligence	Flexibility to network control due to the global vission of the network. Make dynamic changes according to requirements.
Abstraction	The capability to support multivendor devices management and technologies in the infrastructure layer.
Independence	Applications for managing network resources that do not depend on proprietary software.
Use of open standard	Facilitates network design and operation.

B. SDN controllers

As illustrated in Fig. 2, the SDN network's intelligence is (logically) centralized in software-based controllers, which maintain a global vision of it. Network devices delegate the responsibility for managing communications to the controller and become simple traffic relay units.

The controller is a piece of equipment that can convert the SDN applications' requests into orders towards the lower layers' devices and thus provide the SDN applications with an abstract vision of the network. It is responsible for deciding how the packets should be forwarded by one or more network elements and scheduling the network nodes to implement it. Its function is to keep updated the data plane's forwarding tables or infrastructure devices based on the network topology or requests for external services [11].

The SDN controller is in charge of translating the application layer's needs or requirements to the infrastructure layer's network elements through the southbound protocols. It also provides an API (northbound) so that flows can be programmed from the application layer and provide feedback to the application with information on the network topology or packet traffic [6].

The data plane control interface is formalized through the OpenFlow protocol, which has become the official protocol for the remote connection between the SDN controller and the switches. As a result, creating an SDN network should be based on selecting devices and control software that support the OpenFlow standard.

In [12], the main characteristics to consider when evaluating an SDN controller

are presented. Table II summarizes these characteristics for some of the existing open-source drivers. It is worth noting that additional characteristics should be considered, such as:

- Scalability, the number of devices that a controller can support.
- Throughput, the number of flows that the controller can set per second.
- Reliability, ability to discover several paths from origin to destination to ensure availability due to link interruption.
- Network security, controller's ability to support authentication, and authorization.

TABLE II. OPEN-SOURCE SDN CONTROLLER

Characteristic	*Floodlight*	*Ryu*	*ODL*
OpenFlow support	Yes	Yes	Yes
Virtualization	Mininet and Open vSwitch	Mininet and Open vSwitch	Mininet and Open vSwitch
Development language	Java	Python	Java
Graphic interface	Web	Web	Web
Platforms support	Linux, Mac OS, Android	Linux	Linux, Mac OS, Windows
OpenStack support	Yes	Yes	Yes
Multitask	Yes	No	Yes
Time in the market (Years)	8	7	6
Documentation	Good	Average	Average

Due to the characteristics and functionalities, such as being open-source, supporting OpenFlow, Openstack support, popularity, and existing documentation, we evaluate three controllers: ODL, Floodlight, and Ryu.

1) OpenDaylight (ODL) controller: It is an open-source project. It is a driver implemented in the software included within its own Java Virtual Machine (JVM). The project is currently supported by Citrix, IBM, Juniper, Microsoft, VMware, and others. It supports OpenFlow, although it can support other protocols such as BGP. It defines a service level agreement (SLA) that you must adhere to regardless of the controller and network devices' underlying protocol. Its most recent version, Beryllium, includes high availability, clustering, security features, and the improvement or addition of new protocols. The SDN OpenDaylight driver has multiple layers. The upper layer comprises network and business logic applications, the middle layer where the SDN abstractions are located, and the lower layer where the physical and virtual devices are located. The middle layer is the framework that houses northbound and southbound APIs. The business logic resides in the applications that are above the middle tier. These applications use the controller to gather network intelligence, run algorithms to perform analysis, and then use the controller to orchestrate the new rules throughout the network [14].

2) Ryu controller: It is an open-source SDN controller designed to increase network agility by making it easier to manage and adapt traffic. The Ryu controller offers software components with well-defined APIs that make it easy for developers to create new network control and management applications. With this component approach, organizations can customize deployments so that specific needs can be satisfied. Developers can promptly and smoothly modify existing components or implement their own to guarantee that the underlying network can meet their applications' changing demands [15]. It supports various protocols to manage devices, including OpenFlow. Its main features are the following:

- Ability to receive and manage events;
- Ability to analyze incoming packets and create new packets to send to the network;
- Ability to create and send OpenFlow messages to reprogram switches.

3) Floodlight controller: It is an open-source SDN controller written in Java. It supports the OpenFlow protocol as a communication interface (southbound interface) with network elements. It is an enterprise-class driver available under the Apache license for almost any purpose and is supported by a large community of developers. Floodlight is designed to work with many switches, routers, virtual switches, and access points that support the OpenFlow protocol [11]. It is a multiplatform system since it works on the Java virtual machine. The Floodlight architecture is modular, with components that include the functionality described in the ODL controller model. It has

ISSN: 1390 -9266 – 2020 LAJC

a web-based user interface and a Java-based graphical user interface, called Avior. It is one of the most documented drivers today.

C. Benchmark tools for controllers' evaluation

In [12], two tools are proposed for evaluating the controllers, namely Cbench and Hcprobe. These tools are very effective in performing performance, scalability, availability, and security tests.

1) Cbench: It is a tool to monitor OpenFlow controllers through the generation of events. Cbench emulates a configurable number of OpenFlow switches that communicate with an OpenFlow controller to measure different aspects of its performance and latency. Its essential operation consists in that each emulated switch sends a configurable number of new flow messages (OpenFlow packet-in messages) to the OpenFlow controller, waiting for the appropriate flow configuration responses (OpenFlow packet-out messages or OpenFlow messages for modification of flow-mod flows) and records statistics of the time difference between requests and responses, as well as other performance metrics.

2) Hcprobe: It allows for creating scenarios for SDN control tests quickly. It is capable of simulating a large number of switches and hosts connected to a controller. By using Hcprobe, various controller performance indices can be flexibly tested and analyzed. It allows specifying patterns for generating OpenFlow messages (including malformed ones), setting the traffic profile, among others. It is written in Haskell and allows users to create their driver testing scenarios easily. The key features of the Hcprobe are:

- Generation of OpenFlow packages;
- API for designing custom tests;
- An embedded domain-specific language (eDSL) for creating tests.

Besides, Hcprobe provides the framework for creating several test cases to study the behavior of OpenFlow controllers processing different types of messages. It can generate all kinds of messages and reproduce different communications scenarios, even the most sophisticated ones, which cannot be easily reproduced using hardware and software OpenFlow switches. It is useful for developers to conduct driver security testing, regression, and functionality [16].

IV. EXPERIMENTAL SETUP

An ASUS ZenBook computer, with a 2GHz Intel Core i7 processor and 8 GB of RAM was used to make a quantitative comparison between SDN controllers. In this equipment, the Oracle VM VirtualBox tools and a virtual machine were installed using Ubuntu 14.04.06 operating system with 4096 MB of RAM. The drivers to be evaluated were installed on this virtual machine and the Mininet emulator and the Wireshark protocol analyzer with support for OpenFlow, which were used to check the drivers' operation.

We use Mininet to prototyping large networks on a single computer. It is used to create software-defined networks using lightweight virtualization mechanisms. These features allow Mininet to create, interact, customize, and share prototypes quickly. The prototypes should be easily shared with other collaborators, who can run and modify the experiments [17]. Mininet networks run real code, including standard Linux kernel and network applications. Notably, a Mininet-running design can usually go straight to physical switches. It is worth mentioning that different network topologies can be created.

As explained, SDN controllers have different properties, as well, the choice must be subjected to a multi-criteria decision-making process, depending on what characteristics they have and the scope in which they will be implemented. The tests carried out are performance calls; they aim to measure latency, data transfer rate (throughput), and scalability. Latency is defined as the time that a controller needs to respond to a request and is measured in seconds. The transfer rate is the number of transmissions the controller can handle measured in flows/second. Finally, scalability will be measured as the controller's performance against increasing network size and measured as flows/second for a different number of switches in the network. Both for the latency and throughput evaluation, Cbench values of 10,000 hosts and 16 switches are used. For scalability, the number of switches used is varied. In the three test scenarios carried out, the environment presented in Fig. 3 is used, the controller will be ODL, Ryu, or Floodlight.

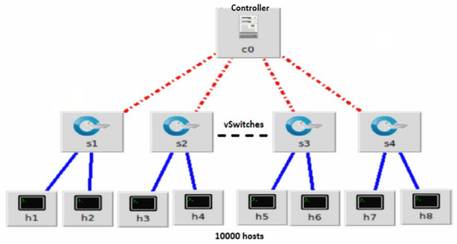


Fig. 3. Experimental Setup

The Cbench benchmark was used to conduct the performance evaluation. Each Cbench run consists of 20 test loops with a duration of 10 secs. We take an average of five runs of each experiment as a result.

V. RESULTS

The obtained results are presented in this section, considering the evaluated parameters: latency, throughput, and scalability.

A. Latency

This test allows a comparison of the latency introduced by different controllers running a learning switch application. For this test, we must use Cbench in latency mode. In this mode, each switch requests a new flow (OFPT_PACKET_IN) and waits for the response (OFPT_PACKET_OUT or OFPT_FLOW_MOD) before requesting the next request. This mode measures the controller processing time in low traffic conditions. In (1), the command to execute Cbench in latency mode is presented; for a driver running on the local machine on port 6633, it must be understood that the drivers, Cbench, and all its add-ons were correctly installed [18].

root@edh-VirtualBox:/openflow/ofloops/cbench# cbench- c localhost -p 6633 -m 10000 -l 10 -s 16 -M 10000 (1)

The results of the average latency obtained can be observed in Fig. 4. Knowing that lower latency is better for the network, it can be seen that the Ryu controller is the one with the highest latency compared to ODL and Floodlight, which have similar latency with a small advantage for ODL that it has an average latency of less than 5 ms. The two drivers can be said to have low latency.

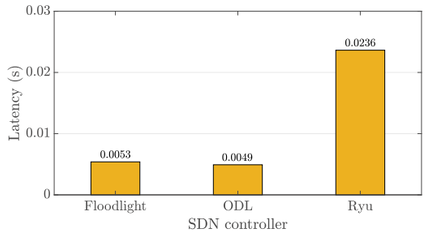


Fig. 4. Average latency per controller

B. Throughput

For this test, Cbench is used in throughput mode (2); the -t option must be added at the end to specify the mode. This mode evaluates the packet flow (number of packets) that the controller can process in a second.

root@edh-VirtualBox:/openflow/ofloops/cbench#cbench-c localhost -p 6633 -m 10000 -l 10-s 16 -M 10000-t (2)

In throughput mode, each switch requests a new flow (OFPT_PACKET_IN) and keeps as many pending requests as its buffers allow. This mode is used to evaluate the maximum rate of establishment of flows that a controller can maintain [11]. Fig. 5 illustrates the controller response's average results to the messages issued by Cbench in throughput mode to evaluate the ODL, Ryu, and Floodlight controllers. Knowing that the higher the throughput, the greater the efficiency in the network, it can be seen that the Floodlight controller has the highest efficiency in the transfer rate, exceeding 90 000 responses per second; below it is OpenDaylight, reaching a throughput of almost 43 450 response packets per second. On the contrary, the Ryu controller is the one that presents the least number of responses per second. That is, it is the one with the lowest throughput that handles only 12865 responses per second.

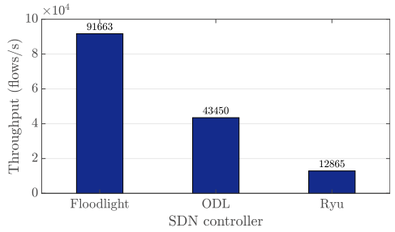


Fig. 5. Average throughput per controller

ISSN: 1390 -9266 – 2020 LAJC

C. Scalability

This test analyzes the network performance when the number of switches is increased, keeping the number of hosts at 10000. We can define scalability as a controller's ability to handle a large number of nodes and accept new nodes without the need for changes or a decrease in network performance. The three controllers' performance in terms of throughput will be compared when the number of switches in the SDN network is increased to perform the scalability evaluation. The tests were carried out varying the size of the network. We used networks with different controllers in a sequence of 4, 16, 64, 128, and 256 switches, respectively. As in the previous cases, the Cbench tool was used with the command shown in (3).

root@edh-VirtualBox:/openflow/ofloops/cbench#cbench-c localhost -p 6633 -m 10000 -l 10-s 256 -M 10000-t (3)

Fig. 6 depicts the average results obtained when evaluating the ODL, Ryu, and Floodlight controllers with Cbench in throughput mode for networks with a different number of switches. As can be seen, the Floodlight controller is the one that performs best when the SDN network has few switches; with four, its performance exceeds 100 000 responses per second, although it is evident that its performance drops drastically when the number of switches is increased to 64 (32 765), then 128 and 256 switches to reach an apparent balance in performance. As far as ODL is concerned, it has a substantial performance drop when increasing the number of controllers from 4 to 16 (87 548 to 43 450 flows per second), from where it can be said that it stabilizes its operation by increasing switches. The Ryu controller starts from low performance, 13 610 responses per second with four switches, a performance that does not drop drastically as the number of controllers increases, although, as observed, it ends with a performance of 1 321 responses/s.

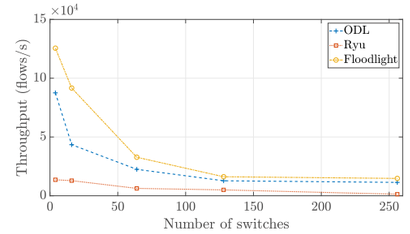


Fig. 6. Scalability evaluation

Finally, an important fact that can be highlighted when choosing a controller is its technical support: the contributions and work that specialized groups dedicated to its development. In this sense, since its appearance in 2013, OpenDaylight has presented a new version each year [19], the result of the lines of code provided by groups of developers sponsored by the "partner" companies, and the users who participate in this community, have a clear advantage over the other controllers as can be seen in Table III. These statistics show that the OpenDaylight community aims at obtaining as soon as possible a reliable, functional, and full-featured platform that will erect itself as the reference SDN controller in the eyes of the entire open-source community.

TABLE III. DEVELOPMENT PER CONTROLLER

	ODL	RYU	Floodlight
Source lines of code	*2'500.000*	*116.000*	*100.000*
Development time (years)	*3*	*4*	*4*

VI. CONCLUSIONS

Benchmarking the performance of a controller is a difficult task. In this work, we qualitatively and quantitatively compare three controllers. With the Cbench tool, it has been possible to compare latency, performance, and scalability between three open-source protocols such as OpenDaylight, Ryu Controller, and Floodlight. The results clearly show that the Ryu Controller presents high latency, low performance, and an inadequate response to small networks and networks with many switches, so its implementation is not recommended. Regarding the Floodlight controller, it shows an acceptable latency response, the best response throughput of packets per second, but it can be observed that in networks with a large number of switches, its performance decreases considerably. In this context, its

implementation in small SDN networks can be recommended. OpenDaylight has low latency, the lowest compared to the controllers studied; its performance is acceptable. Although it has a decreasing performance in scalability, when reaching 64 switches, this tends to stabilize and presents good scalability. It is recommended its deployment in networks with a large number of switches or a growth trend. Both OpenDaylight and Floodlight are Java-based and suffer from inherent bugs and problems with the language. For example, in both throughput and latency modes, Cbench sometimes does not provide results, displaying a "controller disconnected" message, displaying only zeros in the output, or even exiting the Cbench loop without finishing the calculations.

VII. FUTURE WORK

We plan to evaluate additional SDN controllers using other driver performance measurement tools such as Qperf, Hcprobe, or Pktblaster. Also, we plan to evaluate the management and security issues of the SDN controllers. Note that we used centralized controllers in this study with a common campus topology. Therefore, evaluating distributed controllers' performance in WAN environments and/or data centers is relevant, and it is proposed as future work for the project members.

VIII. REFERENCES

[1] Y. Li and M. Chen. “Software-defined network function virtualization: A survey”, in IEEE Access, vol. 3, pp.2542–2553, 2015.

[2] Open Networking Foundation, “Software definednetworking: The new norm for networks”, ONF White Paper, vol. 2, pp. 2-6, 2012.

[3] S. Higginbotham, “Google launches andromeda, a software-defined network underlying its cloud”, 2014.

[4] M. Latah and L. Toker, “Load, and stress testing for SDN's northbound API”, SN Appl. Sci. 2,vol. 122, 2020. https://doi.org/10.1007/s42452-019-1917-y

[5] C. Laissaoui, N. Idboufker, R. Elassali, and K. El Baamrani, "A measurement of the response times of various OpenFlow/SDN controllers with CBench," 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, 2015, pp. 1-2, DOI: 10.1109/AICCSA.2015.7507203.

[6] L. Mamushiane, A. Lysko and S. Dlamini, "A comparative evaluation of the performance of popular SDN controllers," Wireless Days (WD), Dubai, pp. 54-59, 2018. DOI: 10.1109/WD.2018.8361694.

[7] Y. Li, X. Guo, X. Pang, B. Peng, X. Li and P. Zhang, "Performance Analysis of Floodlight and Ryu SDN Controllers under Mininet Simulator," 2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops), Chongqing, China, 2020, pp. 85-90, DOI: 10.1109/ICCCWorkshops49972.2020.9209935.

[8] O. Salman, I. H. Elhajj, I. A. Kayssi, and A. Chehab, “SDN controllers: A comparative Study”, in 18th Mediterranean Electrotechnical Conference (MELECON), 2016. doi:10.1109/melcon.2016.7495430

[9] D. Rodríguez Herlein, N. Talay, C. González, L. Marrone, “Explorando las redes definidas por software (SDN)”, in XXII Workshop de Investigadores en Ciencias de la Computación, 2020. http://sedici.unlp.edu.ar/handle/10915/103546

[10] G. Salazar and L. Marrone, “SDN– Redes Definidas por Software”, 2019.

[11] Y. A. Marín Muro, “Plataforma de pruebas para evaluar el desempeño de las redes definidas por software basadas en el protocolo Openflow”, PhD thesis, Universidad Central "Marta Abreu" de Las Villas. Facultad de Ingeniería, 2016.

[12] A. García Centeno, C. M. Rodríguez Vergel, C. A. Calderón, and F. C. Casmartiño Bondarenko, “Controladores SDN, elementos para su selección y evaluación”, Revista Telemática, vol. 13, no. 3, pp.10–20, 2014.

[13] Open Networking Foundation, “SDN Migration Considerations and Use Cases”, ONF Solution Brief, 2014.

[14] Z. K. Khattak, M. Awais, and A. Iqbal, “Performance evaluation of opendaylight SDN controller”, in 2014 20th IEEE international conference on parallel and distributed systems (ICPADS), 2014, pp. 671–676.

ISSN: 1390 -9266 – 2020 LAJC

[15] G. V. Sánchez Guindulain et al., “Aplicación de SDN para el control del tráfico de red en base a usuarios”, 2017.

[16] A. Shalimov, D. Zuikov, D. Zimarina, V. Pashkov, and R. Smeliansky, “Advanced study of SDN/OpenFlow controllers”, in Proceedings of the 9th Central & Eastern European Software Engineering Conference, 2013, pp. 1–6.

[17] R. L. Santos De Oliveira, C. M. Schweitzer, A. A. Shinoda, and L. Rodrigues Prete, “Using mininet for emulation and prototyping software defined networks”, in 2014 IEEE Colombian Conference on Communications and Computing (COLCOM), pp. 1–6, 2014.

[18] K. Phemius and M. Bouet, “Monitoring latency with OpenFlow”, in 9th International Conference on Network and Service Management (CNSM 2013), pp. 122–125, 2013.

[19] R. Farre, “Opendaylight: Beryllium released”, 2016 [online] Available: https://blog.rojerfarre.com/2016/02/22/opendaylightberyllium-released/. [Accessed: Sep. 25, 2020].

AUTHORS

Daniel Haro Mendoza

Received the Electronic and Computer Engineering degree from Escuela Superior Politécnica de Chimborazo, Ecuador (2005), the M.Sc. degree in Networking from Escuela Superior Politécnica de Chimborazo, Ecuador (2009), student of the Doctorate of Informatic Science at the Universidad Nacional de La Plata, Argentina since 2018. He was Director of Technologies of Escuela Superior Politécnica de Chimborazo (2014-2015) and Universidad Nacional de Chimborazo (2016-2019). He is currently an Associate Professor with the Universidad Nacional de Chimborazo.

Luis Tello Oquendo

Received the Electronic and Computer Engineering degree (Hons.) from Escuela Superior Politécnica de Chimborazo, Ecuador (2010), the M.Sc. degree in Telecommunication Technologies, Systems, and Networks (2013), and the Ph.D. degree (Cum Laude) in Telecommunications from Universitat Politécnica de Valencia (UPV), Spain (2018). He was Graduate Research Assistant with the Broadband Internetworking Research Group, UPV (2013 - 2018) and Research Scholar with the Broadband Wireless Networking Laboratory, Georgia Institute of Technology, Atlanta, GA, USA (2016-2017). He is currently an Associate Professor with the Universidad Nacional de Chimborazo. His research interest includes 5G and beyond cellular systems, IoT, machine learning.

Luis A. Marrone

Received the Electromechanic orientation Electronic Engineering degree (Hons.) from Universidad de Buenos Aires, Argentina (1978). He is currently Vice-Dean of the Faculty of Informatics, researcher and a full member of the board of directors at the Information Technology Laboratory (LINTI) at the Universidad Nacional de La Plata. His research interest includes Computers Networks, Wireless Communications, Traffic Engineering, Wireless Sensor Networks.

ISSN: 1390 -9266 – 2020 LAJC

An implementation of a Virus focuses on Mobile Devices with Android. An Ethical Hacking Event

Implementación de un virus enfocado en dispositivos móviles Android. Un evento de hacking ético

ARTICLE HISTORY

Received 01 October 2020
Accepted 16 October 2020

Carlos Andrés Estrada Vásquez
Department of Computer Sciences
Universidad de las Fuerzas Armadas - ESPE
Sangolquí, Ecuador
caestrada4@espe.edu.ec

Walter Fuertes
Department of Computer Sciences
Universidad de las Fuerzas Armadas - ESPE
Sangolquí, Ecuador
wmfuertes@espe.edu.ec

Amy Rashell Sánchez Cárdenas
Department of Computer Sciences
Universidad de las Fuerzas Armadas - ESPE
Sangolquí, Ecuador
arsanchez5@espe.edu.ec

An implementation of a Virus focuses on Mobile Devices with Android. An Ethical Hacking Event

Implementación de un virus enfocado en dispositivos móviles Android. Un evento de hacking ético

Carlos Andrés Estrada Vásquez
Department of Computer Sciences Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador
caestrada4@espe.edu.ec

Walter Fuertes
Department of Computer Sciences
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador
wmfuertes@espe.edu.ec

Amy Rashell Sánchez Cárdenas
Department of Computer Sciences
Universidad de las Fuerzas Armadas - ESPE
Sangolquí, Ecuador
arsanchez5@espe.edu.ec

Abstract — Mobile devices have become part of daily social life. However, the vulnerabilities of this equipment are widespread, affecting information or damaging the system internally. Within this problem, this research proposes the implementation of a virus that allows affecting the Android victim device focusing on finding the vulnerabilities through penetration tests. The virus was designed through the principle of thread programming to a generation of scripts. Furthermore, the attack on Android devices' vulnerable systems is conducted, applying social engineering techniques. Thus, through imper- ative programming techniques and functional, the access and use have been achieved, given that the virus had classes that allow connection and communication with the device. Each class was developed together so that in this way, there is a precise relationship between them. In this study, Kali Linux, with different Metasploit commands, was used. The proofs of concept were conducted using controlled virtual network environments. For this, a server and a platform were used to use the IP and the Ngrok host, which allows us to generate a link with the application that will violate Android's services and security over secure tunnels. The results show that the operating system tends to be prone to internal damage. At the same time, users can be affected when their security and pri- vacy are compromised. The proposal contributes significantly to a new version of Android's security patches, implementing a malware model that will integrate techniques to mitigate this problem in the future.

Index Terms — Android, computer security, vulnerabilities, pen- testing, Metaseploit.

Resumen — Los dispositivos móviles se han convertido en parte de la vida social diaria. Sin embargo, las vulnerabilidades de este equipo están muy extendidas, afectando la información o dañando el sistema internamente. Dentro de esta problemática, esta investigación propone la implementación de un virus que permita afectar al dispositivo Android víctima enfocándose en encontrar las vulnerabilidades mediante pruebas de penetración. El virus fue diseñado a través del principio de programación de subprocesos para una generación de scripts. Además, se realiza el ataque a los sistemas vulnerables de los dispositivos Android, aplicando técnicas de ingeniería social. Así, mediante técnicas de programación imperativas y funcionales, se ha logrado el acceso y uso, dado que el virus contaba con clases que permiten la conexión y comunicación con el dispositivo. Cada clase se desarrolló en conjunto para que de esta manera, haya una relación precisa entre ellas. En este estudio se utilizó Kali Linux, con diferentes comandos de Metasploit. Las pruebas de concepto se realizaron utilizando entornos de red virtual controlados. Para ello se utilizó un servidor y una plataforma para utilizar la IP y el host Ngrok, lo que nos permite generar un enlace con la aplicación que vulnerará los servicios y la seguridad de Android sobre túneles seguros. Los resultados muestran que el sistema operativo tiende a ser propenso a sufrir daños internos. Al mismo tiempo, los usuarios pueden verse afectados cuando su seguridad y privacidad se ven comprometidas. La propuesta contribuye significativamente a una nueva versión de los parches de seguridad de Android, implementando un modelo de malware que integrará técnicas para mitigar este problema en el futuro.

Palabras clave — *Android, seguridad informática, vulnerabilidades, pentesting, metaseploit.*

ISSN: 1390 -9266 – 2020 LAJC

I. INTRODUCTION

Mobile devices have become part of daily social life. However, these devices' vulnerabilities are varied, affect- ing information or damaging the system internally. While researchers trying to improve security, there are groups of hackers who seek out vulnerabilities in a scheme to intercept the various insecurities.

Attacks on mobile devices are frequent. Today, it is im- perative to seek alternative solutions and understand which users are most affected. In fact, from a particular perspective, those who do not control their information and do not handle protocols to protect what they share are those who have a security cyber-attack. That is almost non-existent or unknown to these users, so it is easy to access personal information with the right tools. In particular, users do not activate the encryption system to protect their mobile devices' confidential data. Besides, they do not know the proper procedure to do it [1].

Unfortunately, with this information in the wrong hands, users are vulnerable to cyber-crime. They become victims of extortion, revenge, financial exploitation, among other possible consequences. Against this background, the follow- ing question arises: How can a virus focus on the Android system be implemented using ethical hacking methods? In this sense, implementing hacking methods and using them ethically against the Android operating system is a complex task [5] since being open-source somehow has a security level for users.

This study explains the use of Kali Linux as a system of attack on Android devices. For this reason, we use different tools to achieve this, such as a server to clone a web page and a backdoor that hides an Android application extension (APK) format inside an image. APK is a compressed ZIP file with a different extension to be opened and inspected using archive software.
The procedure is based on Ngrok as a server to store the attack, so the device is compromised. The Metasploit framework of the Kali Linux is also used, which will act as the primary agent to provide the commands and connect to the previously created host or server. The way the attack is carried out is through social engineering. The APK would penetrate all access to the device, including files, photos, videos, calls, text messages, histories, navigation [3]. It would also activate the device's different peripherals, such as the camera, the microphone, among others. It is possible to start geolocation to know the exact location, thus allowing an attack on the victim.

For this study, also we attacked the LAN, using a con- figuration of the perimeter router that is accessed remotely. Then it connects to the IP network server. We highlight that we have designed a virtual network environment with VirtualBox, which allows us to generate the appropriate space for a simulation of the Kali Linux. It was considered essential to carry out this distribution because it is the most complete for computer security.

Also, we demonstrated the different insecurities that the Android device has. Since it is based on the Linux Kernel, it is more prone to cyber-attacks, especially outside the LAN. The image will be sent through a social network platform, where the victim will be encouraged to open it. It will then generate a direct link to the download, which will run in the background and executed in the same way, without the victim noticing its attack. Risks based on this type of vulnerability [4] can enable information to be stolen from any device as if it were the user's own.

Consequently, real attacks to IP networks act so that services can be lifted through Kali Linux frameworks. One of the main and most used is Metasploit. Because most people use different Android devices, it is a standard system of interest for the hacker community to conduct various outlaw activities, such as identity theft, spying, and phishing. The results show that the operating system tends to be prone to internal damage. At the same time, users can be affected when their security and privacy are compromised. The proposal contributes significantly to a new version of Android's security patches, implementing a malware model that will integrate techniques to mitigate this problem in the future.

This study's main contribution is the implementation of an Android Operating System virus to show the insecurity in Android devices through a variant of a virus called Chip.I, which lets an attacker access smartphones. Furthermore, it encourages us to be aware of the necessity and importance of having an antivirus to protect the terminals of this kind of attack.

The remainder of this document is structured as follows. Section 2 explains the highlighted work done by other researchers, which were the basis of this study. Section 3 mentions the implementation of the test platform, the ele- ments and tools used, and the theoretical basis related to the attacks on Android that support the present study. Section 4 describes the design and implementation of the virus. Section 5 shows the results obtained from the experiment and its discussion. Finally, Section 6 explains the outcomes and proposes future work lines.

II. RELATED WORK

There are several studies where that talk about the de- tection and prevention of malware on mobile devices. It was known that for the year 2017, Android was the most used operating system worldwide [2]. For this reason, the developer community has managed to improve the security of this Operating System throughout its trajectory. To conduct a vulnerability and mitigation analysis, for example, Alawneh [5] demonstrates how they use data mining to detect mal- ware focused on the Kernel level and the performance of the CPU. The information collected is used to create a learning model about suspicious behavior [5]. In another instance, a machine learning-based on Java API is used and the characteristics that allow them to be differentiated into good or bad [6]. It should be noted that there must be an initial attack. However, the techniques go unnoticed by antivirus or detectors, making it more difficult to eradicate them [3]. It is easy to create malicious APKs installed on mobile phones thanks to a series of social engineering tools and techniques and thus access all the stored information, be it contacts, bank details, social networks, emails, among others [4].

The mechanisms used to evade detecting malicious ap- plications for Android are linking with a backdoor. This allows technicians to match the APK with the virus, which is a design and implementation of backdoor [7]. This study shows the persistence and effectiveness of implementing it to be activated and temporarily run and control the device remotely to our benefit. Another case study for analyzing a malicious extension of Android was focused on a specific user, which used reverse engineering to face malware, demonstrating its relevance in strategies to protect the user [8].

The study carried out by [9] mentions the feasibility of pen-testing in android devices, which present an attack test using a Metasploit service. This study contributes to our work through the developed framework and the backdoor principle hidden in the device. The results show access to the databases and files saved on the device, generating an innovative study for android security.

According to the study proposed by [10], the use of the Internet with pen-tester methods is mentioned. This study contributes to our work in a gratifying way, given the use of Metasploit. Also, in the function of the successful results and the demonstration of a framework capable of violating Android devices' security. Also, the authors use Linux as an operating system and tools capable of violating security patches. Its code is based on Java for the connection and contributes to a different virus's innovative reason.

The proposal of [11] shows how using machine learning lets researchers implement a malware detection system. This detection system, called DroidMark, looks for potential sources of data leakage, and returns are built by reverse engineering, an APK file capable of finding. Compared with our work, they were collecting sensitive data through an Android application created with Java, whose accuracy level is 96.88 %.

III. METHODS

This section presents an experimental platform's de- sign and implementation, which will evaluate the different Android systems' insecurity through test devices. In this context, we applied a series of steps to verify that the devices would be successfully attacked, demonstrating the initial hypothesis of this operating system's insecurity with this type of virus called Chip.I.

A. Virtualization platforms

Virtualization allows users to run several virtual ma- chines simultaneously, each with its virtual guest operating system, which shares the same physical computer (Host) [12]. That is, the software and hardware part and its in- teraction creates an external interface for the user, which also provides a cost-effective solution for the next remote hands-on education [13].

Among the virtualization platforms, VirtualBox is a virtualizer available for free and open-source [14]. This platform has been chosen for this project, compared to other platforms, since it allows creating, loading, and managing virtual machines remotely via Virtual Desktop Protocol (VRDP) [15].

B. Experimental Platform Design.

a) Kali Linux. Kali is a Debian-based Linux distribu- tion intended for advanced penetration testing and security auditing [16]. It is the most applied for computer security due to its default installer tools and frameworks. In this study, Kali allows it to be the central penetration platform to the Android device through Metasploit and Msfvenom [16]. It is common used for computer security due to its default installer tools and frameworks. In this study, it was the central penetration platform to the Android device through Metasploit and msfvenom.

b) Android. For 2017, the Android operating system around the world surpassed Windows according to data from StatCounter [2], which shows that it reaches 37.93% of total use, while the second decrease to 37.91%, followed by Ios, MacOs, and Linux. As one of the most used operating sys- tems in the world, based on Linux, open-source, it facilitates the detection of faults quickly, and thus these can be adapted more efficiently for users [17]. It should be noted that more than one billion users use it from 5G to tablet devices as it is customizable, easy to use, and compatible with Google applications.

C. Metasploit

A Metasploit framework is an open-source tool that allows users to execute exploits or attacks on different oper- ating systems from a machine with the Kali Linux operating system. It is integrated into it, whose main objective is oriented on computer security. This platform also allows users to find, exploit, and validate vulnerabilities, where it is usually used to perform pen-testing and offer security audits. The Metasploit Framework can connect to almost all penetration test life cycle stages, making complex tasks more manageable [18].

D. Exploitation settings

Among the exploits' configuration, the best known for these cases were used, the Meterpreter type of payload [19]. It has the necessary facilities when carrying out an exploit. It uses a system of channeled communication and encrypted communications. Also, in this process, the execution time will be increased, and it will be loaded through the network [20]. As part of the framework Metasploit, other scripts used for this research project are msfvenom, which includes msfpayload and msfencode. Them combining functionality to generate a shellcode can be injected into an application APK for android. With the multi-handler tool, it allows receiving connections with Meterpreter, which is why it facilitates the exploitation of a victim system [21].

E. Apache Web Server

The Apache HTTP Server is a project of The Apache Software Foundation, whose objective is to provide a secure server with HTTP services [22], synchronously with HTTP standards, contained in the same HTTP standards. Apache Web Server almost always uses data from MySQL, PHP script language, and others like Python and Perl. The con- figuration is named LAMP (Linux, Apache, MySQL, and Perl / Python / PHP), where it can be developed and deploy in web-based applications. In the present study, this tool is used to create a fake web page by generating a fake IP made by Ngrok, which will download and install the APK in the background [23].

F. Backdoor for Android

This tool is usually used maliciously. However, in this project, it is merely handled for academic and research pur- poses. It is useful to access systems and perform malicious activities without the victim (in this case, Android user) having knowledge or understanding its functionality [24]. This type of Trojan gives access to an infected system where it allows remote control and can deleting or modifying files, executing them, or carrying out activities related to the device's use. In this sense, the backdoor functionalities are incorporated to inject a Trojan, using the social engineering technique, through image concealment.

G. Reverse Engineering with APKtool

Apktool is a powerful software developed by iBot- Peaches; it is part of Kali Linux tools for reengineering Android APK files. Used to send applications to previously unsupported devices [25], which also can be used mali- ciously to hide malware, to another distribution capacity, or otherwise for analysis penetration testing Android appli- cation. Any other application for Android can be broadcast through the Google Play platform. However, since the risk of exposure is known in this case study, it was very likely to be detectable and discarded before affecting the user. So by using social engineering techniques, it avoids being revealed and can go unnoticed, to meet the objective of this practice.

ISSN: 1390 -9266 – 2020 LAJC

IV. IMPLEMENTATION

To understand how Chip. I works, it is necessary to observe the following steps. As a first instance, prepare the working environment, starting with the initialization and use of the Kali Linux virtual machine in VirtualBox and a second virtual machine to start the Ubuntu Server. Next, the virtual network must be initialized to be able to work in a simulated environment. It was required to open the tools and consoles to be used. Then, we proceed to configure the router to work outside the LAN. In the first instance, it must enter the default IP address, in this case, 192.168.1.1, and thus configure it to accept DMZ's parameters. Later, we proceed to download the tool from the Ngrok website, which will allow linking the configuration with Android devices. Besides, the connection is made, and the following commands are executed to detect the link with the android devices (see Fig. 1 and Fig. 2).

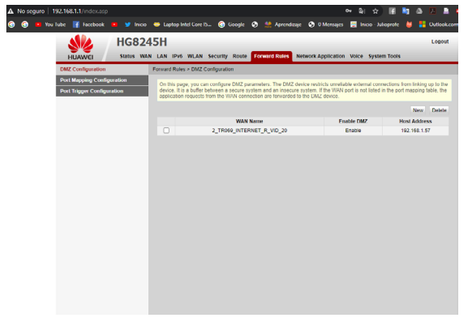


Fig. 1. Login to the router and configure access outside the LAN

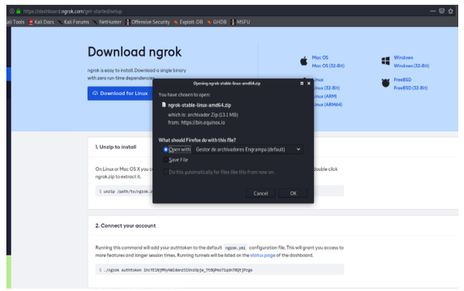


Fig. 2. Download of Ngrok's Package

Afterward, the created Apache2 Web server is initialized, and the previously created web page is accessed through and verification of the link in the virtual machine through the internal NAT network. To verify that the Apache2 page is open, enter the server's IP network, verify that it is running, and create the fake web page (see Fig. 3).

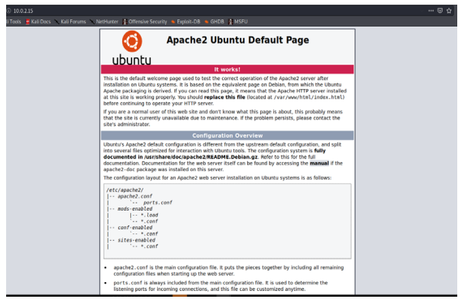


Fig. 3. Access to the created server "Fake web page"

With the following command (see Fig. 4), we call the MSFvenom framework. It was possible to generate and initialize port 4444 and the host, the address, and the appli- cation by creating a package in the format .apk. It allows us to install inside the android device. In this way, we could get access to the data of the victim.

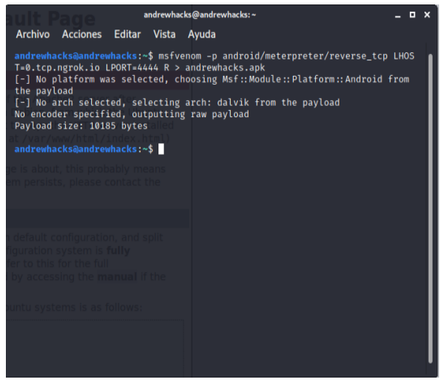


Fig. 4. Creation of the Ngrok package and the APK for Android

As can be observed, the Metasploit was initialized, so it is linked to the console. In this way, access to the required service is obtained. Also, the addresses of the false port are acquired to avoid detections in the LAN network. Thus, we create a false address IP, sharing port 2020 as the central server to the Ngrok platform. When we perform the exploit attack, a reverse TCP

ISSN: 1390 -9266 – 2020 LAJC

attack is carried out, implying to apply social engineering concepts. In other words, instead of the attacker initiating the connection to the device. Once the exploit has been conducted, the Meterpreter is activated.

In the following class diagram (see Fig. 5), it is pos- sible to observe all the attributes. In addition to showing the programming language used, Java users can see the different kinds of data, methods, attributes, and constructors. Whereby the code works is to make a gateway to the appli- cation. As Android is known and its applications work with Java, when establishing a URL connection [26], it passes to the class's established port. It activates the service and the respective SSL validations, also known as certificates.

The main class speaks of MainActivity, which will be re- sponsible for receiving parameters from a Bundle class that creates the connection. It then calls the other methods, in- cluding UrlConnect, which is responsible for connecting the fake web page with the Ngrok server, performing execution, and installation using the Connection class MainService.

V. RESULTS AND DISCUSSION

Once the process is complete, the test is carried out on two terminals. The first is on a device that has Avast antivirus, and the second without any security. Once the attack with Kali Linux is accomplished, the APK file is sent through the WhatsApp social network, achieving to the victim to open the image and be redirected to the false web page's link it is downloaded in the background.

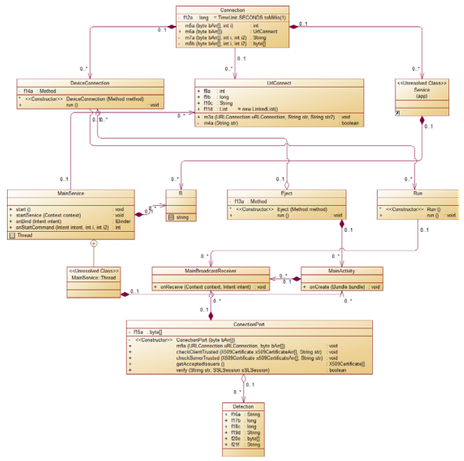


Fig. 5. UML of the APK

As can be seen in the first case (see Fig. 6), the Avast antivirus blocks the installation, preventing it from being carried out and ending the termination of the Chip.I virus. Therefore, an alternative solution is considered to avoid being affected or harmed by data theft, information, and infiltration in the first case. Otherwise, on another device that lacks antivirus security, the application is installed in the background, and the attack is executed. It proceeds to access all the information, and it is installed automatically, which generates a gateway to the server created earlier. The installation has been successful, so the hack performed from the *Meterpreter* exploit.

Once the terminal is accessed, we verify what commands exist and send emails to the victim or text messages. In this way, and at the same time, it can be verified that the hack was successful. Thus, what Meterpreter, as an exploit, allows, is even to remove the call information and observe the conversations that have been had in the different social networks or messaging (see Fig. 7 and Fig. 8).

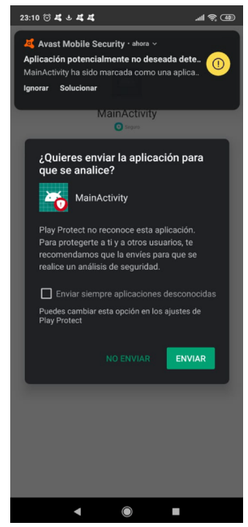


Fig. 6. Installation blocking by avast antivirus

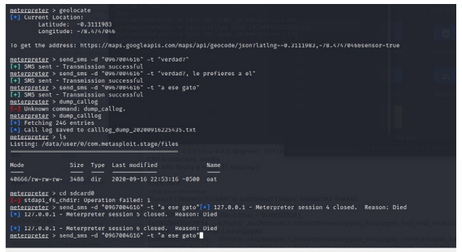


Fig. 7. Management commands in Meterpreter for sending messages and geolocation

The following statistical illustrations show the number of packets received and the transmission and reception band width when the application is active. Also, their performance outside the LAN considers that there is no very high net- work consumption. Figure 9 displays the number of packets received and the time in which they are present, as well as the average transmission or reception speed.

Figure 10 presents the transmitted and received data for the application being executed with the Android device in a pie diagram.

Figure 11 illustrates the received and transmitted data on a timeline, using the bar chart, which indicates that the received packets are more significant due to the amount of data from the attacked device.

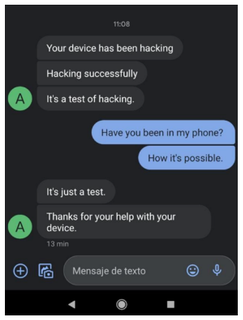


Fig. 8. Verification of the hacking in the another device

When analyzing the network's behavior (see Fig. 12), we deduce that this is due to the large number of packets transferred to the mobile device when the antivirus was disabled. Consequently, during transmission, it is likely to receive any infected information on the system. The network received a large number of packets when the attack was perpetrated. However, when the antivirus was activated, its behavior differed, as it prevented the *Chip's.I* entry virus. After the attack is conducted, the packets received to the virtual machine are greater than those transmitted, which is likely to cause the system to collapse. Figure 12 also depicts the network's behavior when the antivirus detected the Chip.I virus. In this case, at 10:00 p.m., it shows little traffic, and the network is stable without much data received.

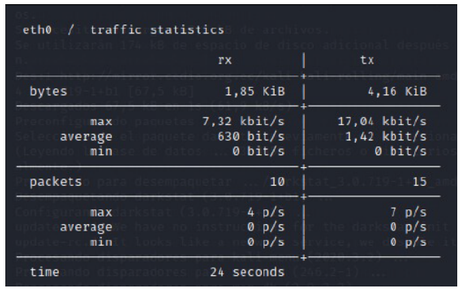


Fig. 9. Statistical data received and transmitted on the network with the application

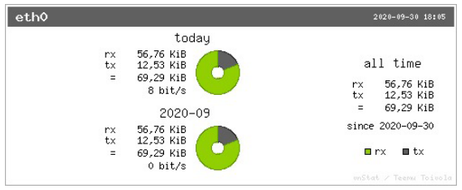


Fig. 10. Pie diagram chart of statistical data

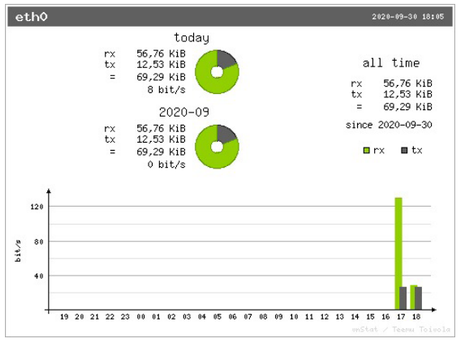


Fig. 11. Bar chart showing the number of packets received by the device

ISSN: 1390 -9266 – 2020 LAJC

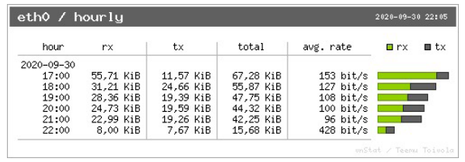


Fig. 12. Bar chart showing the number of packets received by the device

Discussion

After observing that the attack was successful, it is advisable to raise awareness since most of the population uses Android. It can be deduced that the initial Android insecurity hypothesis has been tested as part of the research objective. In this sense, it is stated that having a Linux kernel or having been based on this OS tends to be vulnerable and prone to internal damage. Simultaneously, in the primitive version of Chip.I using the option to affect the peripherals of said server, it was shown that it is possible to overheat the processor and affect its performance. On the other hand, it was also determined that the way it works could be changed, installing the antivirus to make it "invisible," undetectable.

Given that the research gave the expected results, it is confirmed that it was used ethically only for academic purposes. Finally, it should be noted that the controlled virtual network environment, using open source software, can be used to test these devices. As a result, users can be affected by violating their security and privacy, exposing them to the theft of information, their identity, and their credentials, among other possible options. It can even access bank or account details, depending on what the victim has on their terminal.

On the other hand, to perpetuate the attack, it was necessary to access the victim and apply social engineering to convince her to open the image. This image was infected to trick the user into accessing the cloned page through the link inserted in such an image. This method is also known as a backdoor.

For academic testing, it is recommended to have an active server on Apache running Linux, to spoof the desired web page. For the test to be successful, it was necessary not to have any antivirus active or installed. If it existed, the virus to be injected would be detected and automatically eliminated. It is also essential to have the Kali Linux pen- etration test tools, which allow us several options to perpe- trate attacks. Kali Linux is the perfect tool for vulnerability analysis and hackers, who look for cracks in the security of networks and computer systems.

Another aspect that benefited the research was working with port 4444, which uses the Transmission Control Protocol, which is connection-oriented, verifying the link to determine communications from one end to another. Port 4444 guarantees the delivery of data packets in the same order in which they were sent. Once the connection was made, it was necessary to keep the screen active to perform the necessary tests.

Finally, it is confirmed that this study is part of a project created for educational and ethical purposes to detect and mitigate Social Engineering attacks. It is also focused on ex- ploring weaknesses in the security of networks and systems for personal and business use. We use Kali Linux as a tool for forensic analysis, penetration testing, and vulnerability analysis. We try to develop solutions to discover where a computer system has been attacked and find the possible activities carried out by its attacker.

VI. CONCLUSION

This study is focused on demonstrating the vulnera- bilities of the operating systems of mobile devices. Con- sequently, we concluded that the Android system is not safe when installing an APK, and it is vulnerable to being attacked in the form of a backdoor. Thus, it could cause insecurity for users who work with this type of device and damage their integrity, security, and data privacy. It is considered that the Chip.I virus is capable of entering any device with the aforementioned operating system since it is based on the Linux Kernel. It is easily controllable or hack-able, using the commands that were explained during this study. In addition to its easy access to the different types of files, whether hidden or encrypted, also thanks to the tools that Kali Linux has, the attack is more precise and simple through IP networks outside the LAN. Thanks to the different Frameworks such as MSFVenom, Metasploit

through Meterpreter or Ngrok as access server path to it in connection with the Host. So, finally, the research hypothesis is accepted, inferring that the virus is capable of violating security and remaining as a Trojan inside the device, without being detected, unless it has an antivirus, either Avast, AVG, among others, which would be responsible for eliminating it avoiding the attack on the terminal.

As future work, we plan to make a version capable of forcing security and mitigation using Deep Learning to any Android device using a convolutional neural network. Our proposal contributes significantly towards a new version of the security patches for Android in implementing a malware model, which will integrate techniques capable of mitigating it.

ACKNOWLEDGMENTS

The authors would like to thank the financial support of the Ecuadorian Corporation for the Development of Research and the Academy (RED CEDIA) in the development of this study, within the Project Grant GT-Cybersecurity.

VII. REFERENCES

[1] W. Fuertes, F. Meneses, L. Hidalgo, and J. Torres, "RSA over-encryption implementation for networking. A proof of concept using mobile devices", Revista Investigación Operacional, vol. 41, no. 5, Article ID 586598, 2020. Available: https://rev-invope. univ-paris1.fr/fileadmin/rev-inv-ope/files/41420/41420-10.pdf.[Online; Accessed on October 23, 2020].

[2] R. Simpson, "Android overtakes Windows for first time", Statcounter GlobalStats, vol. 3, Abril 2017. Available: https://gs.statcounter.Com8/press/android-overtakes-windowsfor-first-time. [Online; Accessed onSeptember 28, 2020].

[3] M. Costas, "Desarrollo de malware para dispositivos móviles con S.O Android con fines docentes", 2019. Available: http: castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/439/CostasPardoManuel.pdf?sequence=1. [Online; Accessed on September 30, 2020].

[4] M. J. Gutiérrez Fernández, "Inyección de malware en aplicación Android legítima", Universidad de Sevilla, 2019.

[5] H. Alawneh, "Android malware detection using data mining techniques on process control block information", Auburn University, Departament of Computer Science and Software Engineering, 2020. Available: http://hdl.handle.net/10415/7390. [Online; Accessed on September 30, 2020].

[6] A. Pérez, M. Montero y V. Pérez, "Android malware detection using machine learning", en XIII Seminario Iberoamericano de Seguridad en las Tecnologías de la Información, Havana, 2018.

[7] J. Cho, G. Cho, S. Hyun y H. Kim, "Open Sesame! Design and Implementation of Backdoor to Secretly Unlock Android Devices", J. Internet Serv. Inf. Secur., vol. 7, pp. 35-44, 2017.

[8] C. A. Venegas Sánchez, "Using Reverse Engineering to Face Malware", Revista IngenieriaSolidaria, vol. 15, no. 28, 2019.

[9] A. Zadjali, B. Mohammed, "Penetration testing of vulnerability in Android Linux kernel layer via an open network (Wi-Fi)", International Journal of Computer Applications, vol. 975, no. 8887, 2016.

[10] S. Raj and N. K. Walia, "A Study on Metasploit Framework: A Pen-Testing Tool", International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020, pp. 296-302

[11] D. Rathi and R. Jindal, "DroidMa: A Tool for Android Malware Detection using Taint Analysis and Bayesian Network", International Journal on Recent and Innovation Trends in Computing and Communication, vol 6., no 5., pp. 71-76, 2018. Available: https://arxiv.org/ftp/arxiv/papers/1805/1805.06620.pdf [Online; Accessed on October 24, 2020].

[12] W. Fuertes, J. E. López de Vergara, F. Meneses and F. Galán, "A generic model for the management of virtual network environments", IEEE Network Operations and Management Symposium (NOMS)", 2010, pp. 813-816, doi: 10.1109/NOMS.2010.5488367, 2010. https://www.overleaf.com/project/5f720fce6ae2940001a2b161 [Online; Accessed on September 28,2020].

ISSN: 1390 -9266 – 2020 LAJC

[13] P. Li, "Selecting and using virtualization solutions, our experiences with VMware and Virtualbox", Journal of Computing Sciences in Colleges, vol. 25, no. 3, pp. 11-17, 2009.

[14] Oracle, VirtualBox, Available: https://www.virtualbox.org/manual/ch04.html, [Online; Accessed on September 28, 2020].

[15] Oracle, VirtualBox Home Page, Available at: http:// www.virtualbox.org. [On-line; Accessed on September 28, 2020].

[16] Kali, "What is Kali Linux?, Ofensive Security", 2020. Available: https://www. kali.org/docs/introduction/what-is-kalilinux/. [On-line; Accessed on September 28, 2020]."

[17] Rastreator, "Android overtakes Windows for first time", 2020. Available: https://www.rastreator.com/telefonia/articulosdestacados/el-sistema-operativoandroid.aspx, [Online; Accessed on September 28, 2020].

[18] Kali Tools, "Metasploit Pro User Guide", 2020. Available: https://tools.kali.org/exploitation-tools/metasploit-framework, [Online; Accessed on September 28, 2020].

[19] Offensive Security, "About the Metasploit meterprete", 2020. Available: https://www.offensive-security.com/metasploit-unleashed/aboutmeterpreter/, [Online; Accessed on September 28,2020].

[20]Rapid 7, "Using Exploits", 2020. Available: https://docs.rapid7.com/metasploit/using-exploits/, [Online; Accessed on September 28, 2020].

[21] Z. Mohammed, MSFVenom,21 Abril 2020. Available: https://medium.com/@mzainkh/msfvenom-b57267a5bd9d, [Online; Accessed on September 28, 2020].

[22] ApacheCon, "The number one HTTP Server on the Internet, Apache HTTP Server Project", 2020. Available: https://http.apache.org/the-number-one-httpserver-on-the-internet, [Online; Accessed on September 28, 2020].

[23] Ubuntu Server, "HTTPD-Apache2 Web Server", Canonical, 2020. Available: https://ubuntu.com/server/docs/web-serversapache, [On- line; Accessed on September 28, 2020].

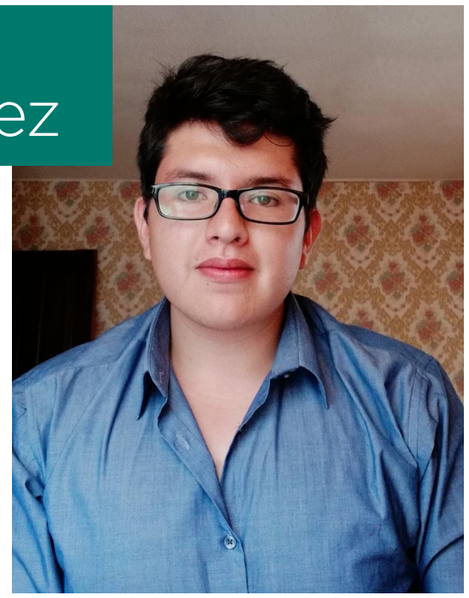
[24] Welivesecurity, "¿Sabes qué es un backdoor y en qué se diferencia de un troyano?", ESET, Abril 2015. Available: https://www.welivesecurity.com/la-es/2015/04/17/quees-un-backdoor/ [Online; Accessed on September 28, 2020].

[25] M. Sweeney, "Decompile and modify APKs on the go with APKTool for Android [XDA Spotlight]", xda-developers, Marzo 2017. Available: https://www.xda-developers.com/decompile-and-modify-apks-on-thego-with-apktool-for-android/ [Online; Accessed on September 28, 2020].

[26] E. Benavides, W. Fuertes, S. Sanchez-Gordon, and M. Sanchez, "Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review", in Rocha A. and Pereira R. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol. 152. Springer, Singapore, 2020. DOI https://doi.org/10.1007/978-981-13-9155-2 5 [Online; Accessed on October 23, 2020].

AUTHORS

Carlos Andrés Estrada Vásquez

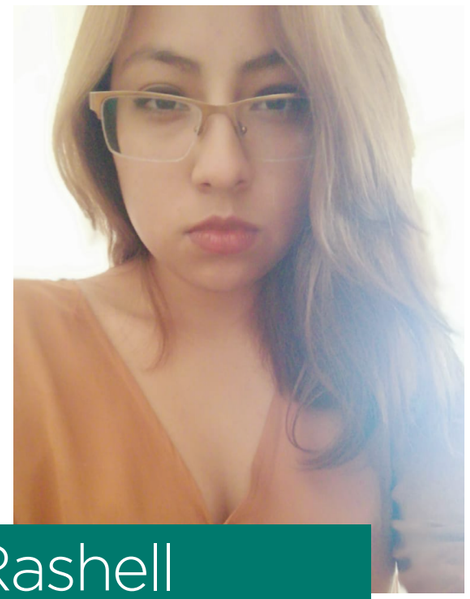


Was born in Quito, Ecuador. Currently, he studies Information Technology Engineering at the Universidad de las Fuerzas Armadas ESPE at Sangolqui-Ecuador. Also, he is a research assistant in the School of Computer Science. Andres is interested in learning and researching by himself in computer science, artificial intelligence, information security, computational mathematics. He has done different courses in Data Analytics and Machine learning through virtual platforms such as Coursera or edX, also he has done courses in computer vision, artificial intelligence, and Python for Data Mining in the Bootcamp IEEE."

Walter Fuertes

Was born in Arenillas, El Oro, Ecuador. Currently, he works at the Universidad de las Fuerzas Armadas ESPE in Sangolquí, Ecuador. He is a full professor (lecturer-researcher) in the School of Computer Science, where he received an engineering degree in Computer Systems in 1995. Later, he received his master's with a science degree in Computer Networking from the Escuela Politécnica Nacional in Quito, Ecuador, in 1999 and the Ph.D. (Hons.) degree in Computer Science and Telecommunications engineering from the Universidad Autónoma de Madrid, Spain in 2010. Since 2006, he has actively participated in several research projects focused on applying virtualization technologies, data sciences, microservice architecture, and cybersecurity. His research interests include managing distributed environments, network security, cybersecurity, the applied research of virtualization technologies, and serious games.

ISSN: 1390 -9266 – 2020 LAJC



Amy Rashell Sánchez Cárdenas

Amy was born in Quito, Ecuador. She is currently studying at the Universidad de las Fuerzas Armadas ESPE in Sangolqui, Ecuador. She is a full-time student at the College of Computer Science, where she is studying to receive an engineering degree in Information Technology. She has a great interest in learning and researching in the different fields of information technologies applied in psychology, computer security, virtual reality, augmented reality, among others.

Procesamiento digital de imágenes en la creación de prototipo de sistema inteligente para detección y reconocimiento de texto en etiquetas de conductores eléctricos recubiertos

Digital image processing in the creation of an intelligent system prototype for text detection and recognition in the labeling process of electrical cable

ARTICLE HISTORY

Received 11 September 2020
Accepted 16 October 2020

Juan J. Navarro
Department of Automation projects
Continuous Improvement Mannagement
Associates S.C.
San Luis Potosí, México
jnavarro@cima.us
https://orcid.org/0000-0002-5674-0265

Carolina Reta
Department of IT, Control, and Electronics
CONACYT-CIATEQ A. C.
Hidalgo, México.
carolina.reta@ciateq.mx
https://orcid.org/0000-0002-0843-129X

Procesamiento digital de imágenes en la creación de prototipo de sistema inteligente para detección y reconocimiento de texto en etiquetas de conductores eléctricos recubiertos

Digital image processing in the creation of an intelligent system prototype for text detection and recognition in the labeling process of electrical cable

Juan J. Navarro
Master's program
CIATEQ A. C.
Department of Automation projects
Continuous Improvement Mannagement Associates S.C.
San Luis Potosi, Mexico
jnavarro@cima.us

Carolina Reta
Department of IT, Control, and Electronics
CONACYT-CIATEQ A. C.
Hidalgo, México.
carolina.reta@ciateq.mx

Abstract — El etiquetado del cable permite identificar distintas configuraciones y lotes de cables, así como conocer sus características. En el proceso de etiquetado del cable se pueden presentar distintos tipos de errores o defectos en el texto impreso, por ejemplo: ausencia de la etiqueta, corrimiento de la tinta, partes del texto faltante, texto ilegible y gotas de tinta. En este trabajo se presenta un prototipo de sistema para la validación del texto en cables eléctricos mediante técnicas de procesamiento de imágenes. El sistema propuesto integra dos etapas. En la primera etapa se propuso un método basado en clusterización por K-means que permite realizar el preprocesado de las imágenes para acondicionarlas. En la segunda etapa se realiza el reconocimiento óptico de caracteres utilizando el motor Tesseract OCR, el cual permite convertir el texto contenido en las imágenes en cadenas de caracteres. La experimentación se realizó utilizando una colección de 909 imágenes de cables eléctricos que contiene ocho tipos diferentes de cables, donde las imágenes están etiquetadas individualmente con la ground truth. La experimentación realizada permitió obtener una tasa de error promedio del 6.54%, 3.97% y 2.53% al validar el texto empleando tres, cinco y siete secuencias de etiquetas, respectivamente.

Keywords — Detección de texto en cables; sistemas inteligentes; procesamiento digital de imágenes; K-means; OCR; Tesseract.

Abstract — *Cable labeling allows identifying different configurations and batches of cables, as well as their characteristics. In the cable labeling process, different types of errors or defects can occur in the printed text, such as the absence of the label, ink bleeding, text parts missing, illegible text, and ink drops. In this paper, a prototype of a system for text validation in electrical cables using image processing techniques is presented. The proposed system consists of two stages. In the first stage, a method based on K-means clustering was proposed, allowing preprocessing images to condition them. In the second stage, optical character recognition using the Tesseract OCR engine is performed, allowing the text in the images to be converted into character strings. The experimentation was carried out using a collection of 909 images of electrical cables containing eight different types of cables, where the images are individually labeled with the ground truth. The evaluation obtained an average error rate of 6.54%, 3.97%, and 2.53% when validating the text using three, five, and seven label sequences, respectively.*

Keywords — *Text detection on cables; intelligent systems; digital image processing; K-means; OCR; Tesseract*

ISSN: 1390 -9266 – 2020 LAJC

I. INTRODUCCIÓN

En el sector industrial de la fabricación de conductores eléctricos poco a poco se van implementando herramientas tecnológicas para lograr su conversión en una Industria 4.0. Dentro de los diferentes procesos que se realizan para la fabricación de cable eléctrico existe el proceso de extrusión[1], en el cual se aplica un recubrimiento plástico o goma sobre un conductor eléctrico. Posterior a esto se etiqueta el producto con base en las especificaciones del fabricante. El proceso de etiquetado puede ser desde grabado por relieve con dados hasta sistemas de impresión por inyección de tinta [2]–[4]. Sin embargo, al depender de tinta o de un dado grabador para el correcto marcaje, en el proceso de etiquetado pueden presentarse problemas como: corrimiento de la tinta, daño en el dado grabador por manipulación incorrecta, impresión errónea del texto debido a una mala limpieza del dado grabador, entre otros.

La problemática principal relacionada con el etiquetado se presenta cuando hay ausencia de etiquetas, implicando la necesidad de volver a realizar el etiquetado del cableado y, por consecuencia, aumentando el tiempo de producción en la línea. Otra problemática es la presencia de la etiqueta con información errónea, generando el tener que desechar el producto por completo o tener que pasarlo a un reprocesado, dependiendo del producto que se esté fabricando. Estas problemáticas aumentan el tiempo de fabricación del producto, alterando la planificación de producción, atrasando a su vez los tiempos de producción de otras líneas o generando desperdicio de material en casos donde no es posible realizar un reprocesado.

Poder realizar la detección y la validación de manera automática de las etiquetas que se graban en el conductor eléctrico, el cual está siendo fabricado por una máquina extrusora, resuelve los problemas de ausencia e impresión con información errónea de las etiquetas, permitiendo a su vez cumplir con estándares de calidad para el producto.

Por lo anteriormente expuesto, desarrollar un sistema inteligente basado en técnicas de procesamiento de imágenes que sea capaz de realizar la detección de etiquetas en las líneas extrusoras de cable eléctrico repercute en una mejora en el control de producción y calidad para este proceso de fabricación; debido a que detectando de una manera rápida y precisa errores en el etiquetado se pueden tomar acciones correctivas en el producto, evitando así que este tenga que ser desechado por completo o reprocesado.

II. ESTADO DEL ARTE

A continuación, se presenta el trabajo relacionado de sistemas OCR (del inglés Optical Character Recognition) aplicados tanto en el reconocimiento de texto en documentos como en sistemas inteligentes de inspección visual de productos; también se presentan distintas técnicas para optimizar la etapa de pre procesado de imágenes y distintos métodos para clasificar caracteres utilizando enfoques de aprendizaje automático.

A. Reconocimiento de texto en documentos

El reconocimiento de texto en los documentos presenta diversas problemáticas que deben abordarse considerando: el área de estudio y tipo de documento con el que se trabaja; el origen; la manera de digitalizarlo; y el tipo de texto que contiene, ya sea impreso o escrito a mano. Dos trabajos destacados que abordan estas problemáticas se presentan a continuación. En [5], utilizando una SVM se procesa el canal que permite obtener mejores características de la imagen de manera automática, combinándolo con un modelo de redes ocultas de Markov para el reconocimiento de palabras. Se obtuvo una precisión del 75.41% en el conjunto ICDAR 2013 [6] y 72.78% en el conjunto de textos propio Devanagari. En [7] se presenta un algoritmo de reconocimiento de caracteres escritos a mano basado en redes neuronales, el cual logra una tasa de reconocimiento de 95.44% utilizando un dataset propio para la evaluación del sistema. Las distintas técnicas utilizadas para el reconocimiento de texto en documentos no son completamente viables para el presente trabajo, debido a que, en la mayoría de estos

casos, el color del texto es contrastante con el color del fondo, situación que no siempre se presenta en el caso de estudio, ya que existen distintos colores de cables, así como colores de etiquetas. En el presente trabajo, para otorgar robustez al reconocimiento de texto en documentos, se utilizó el motor de OCR Tesseract versión 4.0, el cual contiene un algoritmo de reconocimiento basado en redes neuronales.

Los sistemas de OCR pueden aplicarse en: "recopilación de datos bancarios, facturas, documentos legales, incluso en el reconocimiento de números y escritura a mano; también pueden usarse para control de inventario en repositorios institucionales y bibliotecas digitales, reconocimiento óptico de música" [7] y análisis de vulnerabilidades en algoritmos CAPTCHA [8].

B. Sistemas inteligentes de inspección de productos

La inspección visual de productos utilizando sistemas inteligentes, requiere de un desarrollo que sea robusto a las distintas dificultades que se pueden presentar y que pueda trabajar en tiempo real. A continuación, se presentan dos ejemplos de sistemas de inspección basados en reconocimiento de texto.

En [9] se presenta un término importante dentro de los sistemas de reconocimiento de texto, el cual es el OCV (optical carácter verification). Los autores proponen un sistema de clasificación que evalúa el desempeño de la tarea de impresión utilizando algunas medidas de calidad para cada carácter y símbolos. El propósito del sistema es permitir a los clientes la calificación del texto impreso, mientras que, para el fabricante de la impresora, sirve de retroalimentación para la mejora y optimización de su sistema de impresión. Para la parte de clasificación se utilizó un clasificador KNN, basado en el cálculo de la distancia entre cada uno de los caracteres y los caracteres de referencia, obteniendo una tasa de reconocimiento del 98.69% y una precisión del 98.57% en el sistema, utilizando un dataset propio para la aplicación. En [10], los autores presentan un sistema para la detección de las fechas de expiración en envases de alimentos, considerando como crítico el correcto reconocimiento y codificación de esta fecha para una distribución apropiada de los productos, eliminando el posible riesgo a la salud causado por errores en el etiquetado. Se propuso un sistema basado en redes neuronales profundas que incluye a nivel global una red neuronal convolucional para la evaluación de la calidad de la imagen, y una red local completamente convolucional (FCN, del inglés fully convolutional network) [11] para la localización de la fecha. Este sistema obtuvo una precisión del 98% utilizando un dataset propio para la aplicación. En el presente trabajo, el prototipo de sistema inteligente de visión está dirigido a la detección y reconocimiento de etiquetas en conductores eléctricos recubiertos, en donde el texto impreso sobre el conductor está formado en su totalidad por diferentes tomas continuas, por lo que es necesario procesar la imagen que es capturada en su momento. Dentro de los problemas que conlleva este análisis se encuentran: la variación entre el color del texto y el cable; y el tamaño del texto que varía dependiendo del tamaño del conductor eléctrico y del fabricante.

C. Optimización del pre procesado de la imagen capturada

Optimizar la etapa de pre procesado permite mejorar las características de la imagen de entrada al sistema OCR. A continuación, se presenta trabajo relacionado relevante en este tópico.

En [12] se presentan diferentes técnicas para eliminar la variación en el tamaño de los caracteres y la variación en los tonos de grises en el espacio de características antes del entrenamiento del algoritmo de reconocimiento de texto. El cual se divide en dos partes. En la primera parte, el esquema de localización extrae rápidamente los bloques de texto en las imágenes con una tasa de rechazo baja del 0.24%, permitiendo extraer más líneas de texto individuales y normalizar el tamaño del texto. En la segunda parte, se realiza una verificación en un conjunto de espacios característicos, los cuales son invariables a los cambios de escala de grises; para este análisis se utilizó un dataset de las olimpiadas de 1992 en Barcelona, provisto por la BBC[13]. En [14] cada pixel en el área de interés se remplaza por el mínimo local de su vecindario de Moore, mejorando de esta manera la imagen fragmentada por la impresión de inkjet para posteriormente ser validada. En [15] se pre procesa la imagen y se compara con plantillas en una base de datos; una vez realizada la comparación se encuentran los puntos característicos de las imágenes y las características se extraen del área de interés, logrando una precisión del 92% en el reconocimiento de caracteres, utilizando un dataset propio para la aplicación. En [16] se realiza segmentación de caracteres a través de métodos heurísticos, adelgazamiento de la imagen, extracción de características basadas en filtros Gabor y clasificación con SVM; el resultado de este sistema les permitió obtener una segmentación correcta del 97.5%,

ISSN: 1390 -9266 – 2020 LAJC

pero al combinarlo con una clasificación por SVM la precisión para el reconocimiento de caracteres es del 99.4%; en este trabajo se utilizó un dataset propio para la evaluación del sistema. En [17] se realiza reducción de ruido, filtrados Gaussianos pasa bajos, corrección de inclinación con KSC, normalización del tamaño de la imagen, extracción de características con patrones locales binarios y clasificación utilizando el vecino euclidiano más cercano. Se logró obtener en el sistema una precisión del 96.5% al 96.7%, dependiendo del caso, utilizando la base de datos numérica manuscrita de Bangia CMATERdb [18]. En [19] se realiza la detección y corrección de sesgo en el pre procesamiento, la binarización, eliminación de ruido, normalización y el adelgazamiento de las imágenes de entrada. En la extracción de características se obtienen características estructurales dividiendo la imagen en cuatro cuadrantes y características de transformación global obtenidas con la transformada Wavelet, obteniendo 128 características globales y 21 estructurales. En la clasificación se usó una red neuronal y se obtuvo una precisión del 91% para los caracteres y 97.60% para números, utilizando un dataset propio para el experimento. En [20] se utiliza el motor Tesseract, el cual contiene una función que permite asignar una caja o recuadro a cada uno de los caracteres en la imagen; adicionado a esto, se re entrenó el motor utilizando diferentes imágenes en las cuales se varió el tamaño y el tipo de fuente del texto contenido en la imagen. Como resultado se obtuvo una precisión del 81% en la asignación de los recuadros a cada uno de los caracteres, utilizando un dataset propio para el experimento. En [21] se utiliza template matching para extraer las características de la imagen; las cuales se comparan con una base de datos para elegir el carácter con el valor más alto de coincidencia empleando un algoritmo de back propagation. El algoritmo presenta problemas cuando se tienen letras no identificadas, ya que esto conlleva a un resultado erróneo en el reconocimiento del carácter. El algoritmo permitió obtener una precisión del 91.82% en el reconocimiento de caracteres, utilizando un dataset propio para el experimento.

Combinando distintas técnicas de pre procesado, segmentación y clasificación, es posible lograr maximizar los resultados obtenidos de un algoritmo de OCR. En el sistema presentado en este artículo se propone una técnica para mejorar el pre procesado y la extracción de ruido en las imágenes digitales; posteriormente, se utiliza el motor de OCR Tesseract para convertir la imagen a texto; finalmente, se realiza la validación del texto para interpretar si el resultado contiene problemas o errores en el etiquetado.

En la Tabla I se presenta una comparación de las características de algunos trabajos con mayor similitud al propuesto, comparando: espacios de color, la robustez a diferentes situaciones que causan problemas, distintas técnicas para segmentación y métodos de clasificación del texto.

TABLA I. TRABAJO RELACIONADO VERSUS TRABAJO PROPUESTO

Ref.	Espacio de color				Robusto a					Pre procesamiento	Segmentación								Método de clasificación				
	RGB	LAB	Grises	Blanco y Negro	Escala	Interlineado	Objetos en movimiento	Ruido en la imagen	Imágenes de baja calidad	Etapa de pre procesado	Operación Morfológicas	Contornos	Tesseract	SVM	Umbralizado	DNN	K-means	LBP	DNN	HMM	NN	SVM	Tesseract
[7]			x			x	x	x	x	x		x							x				
[5]	x	x	x		x	x			x	x				x						x			
[9]			x					x	x	x	x				x						x		
[10]			x		x				x	x				x		x			x				
[16]	x			x	x					x	x			x								x	
[17]				x	x					x								x	x			x	
[20]				x	x				x				x										x
Propuesto		**x**			**x**		**x**	**x**		**x**					**x**		**x**							**x**

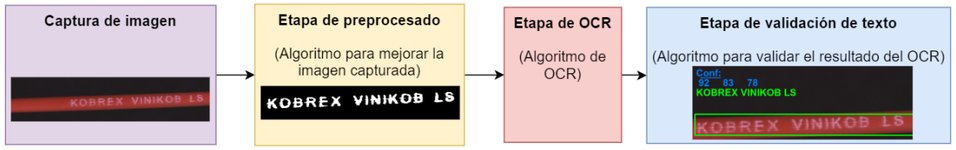


Fig. 1 Esquema del procesamiento digital de imágenes del prototipo de sistema inteligente.

III. MÉTODO PROPUESTO

El sistema propuesto está enfocado en la detección del texto impreso en conductores eléctricos; dicho texto está formado en su totalidad por tomas continuas de imágenes del cable estudiado. Por tanto, es necesario procesar cada imagen capturada en su momento y acumular el resultado obtenido. Dentro de los problemas que conlleva el análisis de las imágenes para la detección del texto se encuentran: la variación entre el color del texto y el cable; y el tamaño del texto que varía dependiendo del tamaño del conductor eléctrico y del fabricante. Para abordar estas problemáticas, en el sistema propuesto se segmenta el texto de la imagen utilizando el algoritmo de clusterizacion de K-means para posteriormente realizar el reconocimiento del mismo. En el sistema propuesto se adopta, por su facilidad de implementación y robustez, la versión 4.0 de Tesseract [22] junto con los paquetes de idiomas de español e inglés; al utilizar esta versión de Tesseract, que utiliza un motor basado en redes neuronales y LSTM, se espera obtener un mejor resultado comparado con el motor de OCR de las versiones anteriores.

El prototipo de sistema inteligente se divide en dos etapas: pre procesamiento y OCR. La Figura 1 presenta los bloques que componen el esquema general del procesamiento y análisis de las imágenes para la inspección de etiquetas en conductores eléctricos. El prototipo permite realizar la validación del texto que se imprime en el conductor eléctrico que se está fabricando mediante una inspección visual. El sistema prototipo funciona de la siguiente manera: una vez capturada la imagen del conductor se realiza un pre procesamiento, el cual permite extraer información propia o característica de la imagen para mejorar su calidad para ingresarla al algoritmo de OCR; posteriormente se utiliza el algoritmo de OCR para convertir la imagen a texto; finalmente, se analiza el texto obtenido del algoritmo de OCR y se valida si el resultado es correcto o erróneo.

La implementación y desarrollo de los algoritmos propuestos en este sistema se realizó utilizando software de fuente abierto: Python [23] y librerías de OpenCV [24].

A. Etapa de pre procesamiento

La etapa de pre procesamiento permite mejorar las características de la imagen de entrada. Para esta etapa se desarrolló un algoritmo basado en el método de clusterización de K-means que integra los siguientes pasos:

*1) Cambio de espacio de color CIE L*a*b**

La imagen de entrada IMG se encuentra en el espacio de color RGB por lo que se realiza el cambio al espacio de color CIE L*a*b*. Este espacio está definido por el conjunto de Ecuaciones 1 [25].

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \leftarrow \begin{bmatrix} 0.412453 & 0.357580 & 0.180423 \\ 0.212671 & 0.715160 & 0.072169 \\ 0.019334 & 0.119193 & 0.950227 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

$$X \leftarrow \frac{X}{X_n} \text{ donde } X_n = 0.950456$$

$$Z \leftarrow \frac{Z}{Z_n} \text{ donde } Z_n = 1.088754$$

$$L \leftarrow \begin{cases} 116 * Y^{\frac{1}{3}} - 16 & Y > 0.008856 \\ 903.3 * Y & Y \leq 0.08856 \end{cases} \quad (1)$$

$$a \leftarrow 500\big(f(X) - f(Y)\big) + delta$$

$$b \leftarrow 200\big(f(X) - f(Z)\big) + delta$$

$$\text{Donde } f(t) = \begin{cases} t^{\frac{1}{3}} & \text{para } t > 0.008856 \\ 7.78t + \frac{16}{116} & \text{para } t \leq 0.008856 \end{cases}$$

$$\text{y } delta \leftarrow \begin{cases} 128 & \text{img de 8 bits} \\ 0 & \text{img punto flotante} \end{cases}$$

$$\text{Imágenes de 8 bits: } L \leftarrow L * \frac{255}{100}, a \leftarrow a + 128, b \leftarrow b + 128$$

En el sistema propuesto solo se utiliza el canal L* correspondiente al canal de luminosidad, permitiendo así reducir el número de canales a procesar. La imagen representada en L* proporciona una mejor variación entre los pixeles claros y obscuros. La imagen obtenida en este paso se denota como como L.

ISSN: 1390 -9266 – 2020 LAJC

2) Clusterización por K-means

Para la extracción del texto contenido en la imagen L se utilizó el método de clusterizacion de k means definido por la ecuacion 2 [26]:

$$argmin(SSE)$$

$$\text{donde } SSE = \sum_{i=1}^{n} \sum_{j=1}^{k} w^{(i,j)} \left\| x^{(i)} - \mu^{(j)} \right\| \quad (2)$$

$$\text{y} \quad w^{(i,j)} = \begin{cases} 1 & \text{si } x^{(i)} \in \text{cluster } j \\ 0 & \text{en caso contrario} \end{cases}$$

En la ecuación 2, $\mu^{(j)}$ es el centroide del cluster j, SSE es la suma de la estimación cuadrática del error y w $^{(i,j)}$ es una variable indicadora que determina la asignación de x^i al cluster j. Este método permite agrupar la información de entrada en grupos y encontrar el centroide de los mismos. El número de clusters define cuantos grupos diferentes se van a generar dependiendo del valor de los pixeles. De manera experimental al elegir tres clusters se busca que cada uno corresponda al fondo de la imagen, al cable y a la etiqueta en el cable, respectivamente; pero al realizar este experimento, existen cables en donde el valor de los pixeles que corresponden al cable y los que corresponden al texto tienen una diferencia de valor pequeña, por lo cual estos valores se agrupan en el mismo cluster, provocando que segmentación del texto contenga pixeles que no corresponden al texto de la etiqueta; esto afecta directamente la posibilidad del sistema de detectar falsos negativos. Al elegir cuatro clusters se busca mejorar el resultado obtenido al elegir tres clusters; añadiendo un cuarto cluster se busca que este cluster contenga los valores que son clasificados erróneamente con 3 clusters; el cluster extra permite asociar a este grupo los pixeles con valor intermedio entre el cable y el texto. Por lo tanto, en este trabajo se usan 4 clusters para disminuir la posibilidad de que el sistema genere falsos negativos.

A los cada uno de los clusters se les asigno el valor del centroide de los pixeles contenidos en los mismos, permitiendo reducir así el número de valores de intensidad. La imagen obtenida en este paso se denotó como IMG$_{kmn}$ y los valores de los centroides se almacenaron en la lista Values=[C_1,C_2,C_3,C_4], para su uso posterior; en Values los valores se encuentran ordenados por intensidad, de menor a mayor.

Para determinar el valor correspondiente al texto en la imagen se propuso la ecuación 3, la cual considera dos casos; cuando el fondo de la imagen es claro, se tiene texto obscuro y en el caso contrario, al tener un fondo de imagen obscuro, se tiene un texto claro.

$$text_{val} = \begin{cases} Values\ [0] & \text{cuando } \frac{\sum_{i=0}^{10} \sum_{j=0}^{10} L_{chan}[i,j]}{10} \geq 200 \\ Values\ [3] & \text{en caso contrario} \end{cases} \quad (3)$$

Con el valor correspondiente al texto se realizó una umbralización utilizando el valor de text_val definida por la ecuación 4:

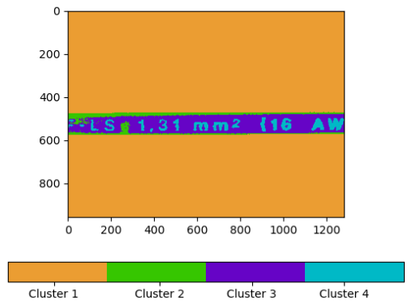


Fig. 2 Resultados del clusterizado, cada grupo está representado con un color distinto

$$mask_{kmn}(x,y) = \begin{cases} 0 & \text{cuando } IMG_{KMN}(x,y) \neq text_{val} \\ 255 & \text{en caso contrario} \end{cases} \quad (4)$$

El segmento que contiene al texto en la imagen original IMG es extraído utilizando la máscara mask_kmn a partir de la ecuación 5:

$$IMG_{text}(x,y) = \begin{cases} IMG(x,y) & \text{si } mask_{kmn}(x,y) = 255 \\ 0 & \text{en caso contrario} \end{cases} \quad (5)$$

En la Figura 2 se presenta una representación visual de los distintos grupos obtenidos al utilizar la clusterización por K-means. En la parte inferior se presenta la barra de color que define el cluster, cada uno marcado con un color distinto.

3) Suavizado de la imagen utilizando un filtro de mediana.

El suavizado de la imagen *IMGtext* se realizó utilizando un filtro de mediana [27], permitiendo reducir pequeños puntos de ruido generados por el paso anterior. Este ruido corresponde a los bordes del texto, en donde dependiendo de la calidad de la impresión pueden presentarse bordes borrosos o difuminados y segmentos internos del texto difuminados; esto genera un borde irregular con recorte en el texto. Una de las recomendaciones para el adecuado funcionamiento del motor OCR Tesseract es suavizar la imagen de entrada al OCR [28]. El valor de *IMGtext* se actualiza con los datos de la imagen suavizada.

La Figura 3 presenta un ejemplo del resultado obtenido de la etapa de pre procesamiento utilizando el K-means

Fig. 3 Resultado de la etapa de pre procesamiento utilizando K-means.

En la Figura 3, es posible observar el resultado de la etapa de pre procesado, la cual permite segmentar el texto correspondiente a la impresión en el cable, removiendo el fondo y el cable de la imagen.

B. Etapa de OCR

Los algoritmos de OCR permiten convertir el texto en una imagen a caracteres (códigos de 8 bits, como los representados en tablas ASCII). El motor o algoritmo OCR adoptado es el motor Tesseract OCR.

La imagen IMG_{text} antes de ser ingresada al motor OCR es umbralizada de manera automática utilizando el método de Otsu [29], debido a que al ser un método de umbralizado automático permite separar la información de IMG_{text} en dos clases. Estas clases se definen en la ecuación 6:

$$IMG_{bin}(x,y) = \begin{cases} 255 & \text{cuando } IMG_{text}(x,y) > thr \\ 0 & \text{en caso contrario} \end{cases} \quad (6)$$

Donde x y y corresponden a las coordenadas de la imagen, thr corresponde al valor límite obtenido del método de Otsu. Por lo tanto, IMG_{bin} corresponde a una imagen binaria en donde los valores mayores a thr se convierten a blanco (255) y los valores menores se convierten a negro (0).

Para mejorar el resultado a obtener del motor OCR se configuraron algunos parámetros del mismo. Existen diferentes formas de analizar la imagen de entrada. Tesseract permite utilizar distintos modos de segmentación de páginas: en una región pequeña, texto contenido en un círculo, texto escaso; dentro de estas opciones se eligió como método de segmentación el método de segmentación automático, sin OSD (Optical Script Detection, en español detección óptica de escritura/fuente).

A partir de la versión 4.00 de Tesseract se incluye un motor de reconocimiento basado en redes neuronales utilizando LSTM, que ofrece una precisión significativamente mayor en las imágenes con texto, por lo tanto, este modo de trabajo del motor OCR fue seleccionado, utilizando a la par los modelos de lenguaje español e inglés.

Para mejorar el reconocimiento del texto contenido en las imágenes, se deshabilitó el diccionario de Tesseract y se creó una lista blanca con los caracteres a detectar: *"0123456789abcdefghijklmnopqrstuvwqyzABC DEFGHIJKLMNOPQRSTUVWQYZº()-./,[]".*

Teniendo los parámetros optimizados para este análisis, la imagen IMG_{bin} se procesa en el motor OCR, obteniendo de él los datos presentados en la Tabla II.

TABLA II. DATOS OBTENIDOS DEL MOTOR OCR

Dato	Descripción
Level	Nivel jerárquico de la palabra en la imagen del 1 al 5, (1 – pagina, 2 – bloque, 3 – párrafo, 4 – línea, 5 – palabra).
Page_num	El número de página cuando se ingresa más de una imagen.
Block_num	El número de bloque dentro de la página.
Par_num	El número de párrafo dentro del bloque.
Line_num	Número de línea en el párrafo.
Word_num	El número de palabra dentro de la línea.
Left	Coordenada X en pixeles de la esquina superior izquierda del rectángulo delimitador de texto, comenzando desde la izquierda de la imagen.
Top	Coordenada Y en pixeles de la esquina superior izquierda del rectángulo delimitador de texto.
Width	Ancho del rectángulo delimitador del texto en pixeles.
Height	Altura del rectángulo delimitador en pixeles.
Conf	Valor de confianza de 0 a 100 (menor a mayor confianza), -1 para todos los niveles excepto el nivel 5 correspondiente a la palabra.
Text	Texto detectado

(a)

(b)

Fig. 4 Resultado del motor OCR. (a) Imagen con fondo claro y texto obscuro; (b) imagen con fondo obscuro y texto claro.

ISSN: 1390 -9266 – 2020 LAJC

De los datos presentados en la Tabla II, obtenidos como resultado del OCR , se utilizaron: el número de palabras y las coordenadas de los vértices del rectángulo delimitador alrededor de la palabra, calculadas a partir de left, top, width y height. Con estas coordenadas se realiza el cálculo para obtener un rectángulo dentro del cual se encuentran todas las palabras reconocidas; la confianza de la predicción y la predicción del texto de la imagen, la cual está representada como una cadena de caracteres.

La Figura 4 presenta ejemplos visuales de resultados obtenido por el sistema. Se presenta la información resultante del motor OCR, en orden de aparición superior a inferior representan: la certeza de cada una de las palabras; las palabras obtenidas y agrupadas en una sola cadena de texto; y el rectángulo que contiene a todas las palabras.

C. Etapa de validación

Los algoritmos de OCR permiten convertir el texto en una imagen a caracteres (códigos de 8 bits, como los representados en tablas ASCII). El motor o algoritmo OCR adoptado es el motor Tesseract OCR.

Para validar el texto obtenido por el OCR se desarrolló un algoritmo diseñado específicamente para el caso de estudio, ya que la etiqueta a detectar está formada por una secuencia de imágenes, en donde en cada imagen de la secuencia se encuentra una sección o segmento del texto.

Bajo este enfoque el algoritmo se desarrolla alrededor de un vector de ceros, representado en la Ecuación 7:

$$\mathrm{A} = [0_0 \quad 0_i \quad \cdots \quad 0_{m-1}]_m \quad (7)$$

En donde m corresponde a la cantidad de caracteres contenidos en el texto real de la etiqueta. Cada producto contiene una longitud distinta. Se considera un carácter válido solamente si se encuentra en la posición correcta y el caracter es el mismo que el analizado, como se representa en la Ecuación 8:

$$\text{Si } C = A_i \ \wedge i_c = i_A \text{ entonces } A_i = 1 \quad (8)$$

En donde C corresponde al carácter a revisar; A_i corresponde al carácter del vector en la posición i, i_c corresponde a la posición del carácter c e i_a corresponde a la posición del carácter en el vector A.

Al finalizar una secuencia de imágenes, los caracteres que no se validaron, se mantienen en cero, representando un error en el etiquetado y permitiendo de esta manera encontrar problemas o defectos en el etiquetado y especificar los caracteres en los cuales se están teniendo problemas.

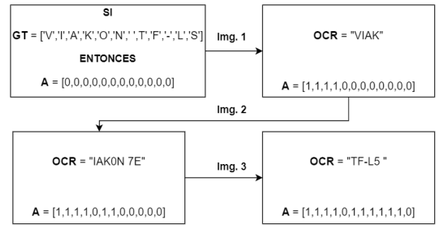


Fig. 5 Ejemplo de la etapa de validación.

En la Figura 5 se presenta un ejemplo de la etapa de validación y la forma en que se va rellenando el vector A. Se presenta un diagrama de bloques en el cual se realiza una pequeña simulación del funcionamiento de la etapa de validación, como entrada se tiene que el ground truth de la etiqueta es "VIAKON TF-LS" por lo tanto el vector A forma un vector de ceros de tamaño 12, que es el número de caracteres contenidos en la etiqueta, considerando el espacio. Al procesar una primera imagen se obtiene un resultado del motor OCR, este resultado corresponde al texto en la imagen; en este primer resultado se obtuvo el texto "VIAK" que corresponde a los primeros cuatro caracteres de la etiqueta, por tanto, el vector A cambia su valor a 1 en las primeras cuatro posiciones. En la siguiente imagen que es procesada, el resultado obtenido por el OCR contiene tres caracteres erróneos, por lo tanto, a pesar de coincidir con la posición correcta, al no ser el mismo carácter que el de la etiqueta, el vector A mantiene el valor de 0 en esa posición. Finalmente, al procesar una tercera imagen el motor de OCR reconoce bien los caracteres detectados anteriormente de manera errónea, por lo tanto, estos caracteres se pueden validar y el vector cambia a 1 en la posición correspondiente a estos caracteres.
Para reducir la posibilidad de generar falsos positivos, se decidió utilizar un número impar de secuencias, combinando el resultado obtenido de una secuencia impar con el resultado de la secuencia impar anterior.

IV. RESULTADOS

A. Base de datos de imágenes

Para realizar la experimentación del sistema prototipo se creó una base de datos formada por diferentes cables. La Tabla III presenta las características de cada uno de ellos. El total de imágenes para realizar pruebas es de 909 imágenes, formada por 8 distintos tipos de cable.

TABLA III. BASE DE DATOS PARA DESARROLLO DEL ANÁLISIS EXPERIMENTAL

Fabricante	Color del cable	Color del texto	Calibre	Núm. de imágenes	Imágenes con texto	Alias
Indiana	Rojo	Negro	12 AWG	74	60	Indiana Rojo
Kobrex	Azul	Blanco	14 AWG	71	54	Kobrex Azul
Kobrex	Rojo	Blanco	16 AWG	130	98	Kobrex Rojo
Kobrex	Rojo	Blanco	14 AWG	87	65	Kobrex Vinikob
Viakon	Blanco	Negro	16 AWG	114	82	Viakon Blanco
Viakon	Negro	Blanco	14 AWG	123	97	Viakon Negro
Viakon	Azul	Negro	18 AWG	94	81	Viakon UL
Viakon	Verde	Negro	14 AWG	216	170	Viakon Negro
Imágenes totales				**909**	**707**	

La base de datos está compuesta por cables que pueden ser similares en cuestión de color, el color del texto, el tipo de cable y el calibre; estas características son similares a las que se usan con mayor frecuencia en Planta. La base de datos contiene información variada que permiten evaluar el método propuesto en distintos casos. Cabe recordar que las imágenes incluyen características o problemas, entre ellos se encuentran: suciedad en la impresora, desgaste o tallones en el cable, material de fabricación con mucho reflejo, corrimiento de tinta o gotas de tinta, y secciones del texto o partes de letras no impresas. El texto impreso sobre el conductor está formado en su totalidad por diferentes tomas continuas, por lo que para la validación del texto se utiliza una secuencia de imágenes.

B. Etiquetado de imágenes con la ground truth

Para cada una de las imágenes de la base de datos se generó un archivo de ground truth, el cual representa el texto real contenido en la imagen. Esta permite realizar una evaluación del desempeño del método propuesto contra el texto real contenido en cada imagen. El proceso de creación del ground truth se realizó de manera manual generando un archivo de texto, el cual contiene el texto contenido en la imagen.

Para mejorar los resultados obtenidos por el motor de OCR se decidió declarar un carácter comodín al principio o al final del ground truth, ya que, dentro del proceso de captura de la imagen, se puede cortar alguna de las letras iniciales o finales del texto. Por lo que, realizar el análisis o la predicción del OCR sobre texto con segmentos incompletos en algunas letras, se considera una situación fuera de lo esperado para el motor OCR, afectando directamente a la precisión de la detección.

C. Evaluación del desempeño del método

Para evaluar el desempeño del sistema se obtuvieron los aciertos por colección y método. A partir de los aciertos o verdaderos positivos por colección se calculó el error en las colecciones y se determinó un error global. La Tabla IV presenta los resultados de dicho análisis y en la Figura 6 se presentan gráficamente estos resultados.

TABLA IV. PORCENTAJE DE ERROR EN LAS DISTINTAS COLECCIONES POR SECUENCIA

	Método K-means % error por secuencia[a]							No. de caracteres en etiqueta
Conjunto	*Sec. 1*	*Sec. 2*	*Sec. 3*	*Sec. 4*	*Sec. 5*	*Sec. 6*	*Sec. 7*	
Indiana rojo	8.93	3.30	2.56	1.98	1.37	0.73	0.00	91
Viakon blanco	8.94	1.00	0.00	0.00	0.00	0.00	0.00	50
Kobrex azul	51.81	36.75	29.26	24.30	20.24	16.87	13.25	83
Kobrex rojo	8.81	4.73	3.35	2.76	2.44	2.44	2.44	41
Kobrex Vinikob	32.53	14.22	6.16	2.26	0.69	0.40	0.00	83
Viakon negro	12.73	6.19	3.74	2.72	1.95	1.66	1.44	87
Viakon UL	20.22	8.29	6.47	5.39	4.41	3.36	2.70	68
Viakon verde	5.12	1.31	0.80	0.73	0.64	0.54	0.43	87
Prom.	18.64	9.47	**6.54**	5.02	**3.97**	3.25	**2.53**	

[a] *Una secuencia contiene la totalidad de imágenes con fragmentos de texto, con los cuales se forma la etiqueta del producto.*

En la Tabla IV y en la Figura 6 es posible observar que al utilizar un mayor número de secuencias la tasa del error disminuye. El utilizar más de una secuencia permite confirmar que el error puede ser decrementado hasta un porcentaje que permita tener el menor número de falsos negativos y validar de manera certera el etiquetado en el cable.

ISSN: 1390 -9266 – 2020 LAJC

V. DISCUSIÓN DE LOS RESULTADOS OBTENIDOS

En la experimentación realizada se observó que el sistema inteligente propuesto tiende a tener problemas en los productos donde la etiqueta del cable no está completamente coloreada del color de la tinta; ya que por su principio de funcionamiento puede llegar a agrupar erróneamente pixeles que corresponden al texto como pixeles del cable o del borde de la impresión. Por lo contrario, en los casos donde la impresión tiene un relleno uniforme, el sistema permite remover el borde de la impresión si es que el texto se empieza a hacer borroso, asignando estos pixeles como otro grupo distinto al del texto, dependiendo del producto a validar.

Debido a que la etiqueta que es colocada en el conductor eléctrico está segmentada en un grupo de imágenes, se compararon resultados que utilizan una sola secuencia de imágenes contra un número mayor de secuencias. En esta comparación fue posible observar una disminución en el error; sin embargo, se tiene un incremento en el número de imágenes necesarias para realizar la validación del texto. De igual manera, cuando el texto validado contiene problemas de etiquetado, fue posible observar que el error deja de disminuir a lo largo del incremento de las secuencias.

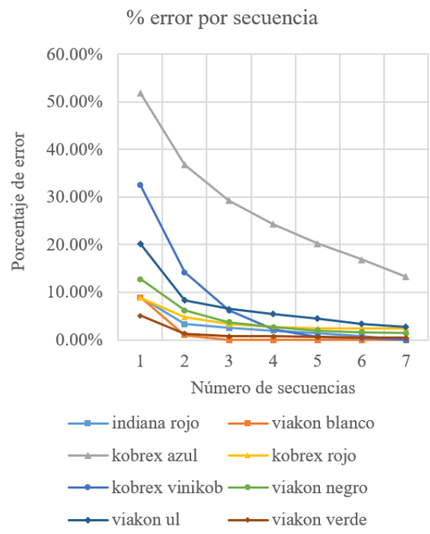


Fig. 6 Porcentaje de error por secuencia en las distintas colecciones.

VI. CONCLUSIONES

En el procesamiento digital de imágenes para la creación del prototipo de sistema inteligente propuesto se empleó el método K-means para agrupar el texto, el cable y el fondo en tres distintos grupos, pero, fue necesario considerar un cluster extra, el cual pudiese clasificar de manera correcta el borde del texto o los componentes correspondientes al ruido, y así permitir segmentar el texto de la imagen original. El sistema propuesto funciona bien en aquellos cables en donde la iluminación genera brillo o sombras en el cable, y en donde el color del texto y el cable es contrastante, tolerando inclusive aquellos cables en donde el borde puede estar un poco borroso. Sin embargo, presenta desventaja cuando el texto es moderadamente borroso o se presentan tallones en el cable. La etapa de pre procesado permitió mejorar las características de la imagen que se ingresa a la etapa de OCR, buscando disminuir la tasa de error producida en la detección del texto; sin embargo, el tamaño del texto, el contraste del texto con el fondo de la imagen y los bordes del texto representan parámetros que pueden mejorar o afectar el resultado del OCR.

En el caso de estudio presentado, la etiqueta que es colocada en el conductor eléctrico está segmentada en un grupo de imágenes; el algoritmo desarrollado permite conocer cuáles caracteres son los que no se pudieron validar a lo largo de la secuencia de imágenes y evitar falsos positivos, ya que los requisitos para que el texto sea validado contra el del ground truth son dos: la posición y la igualdad del carácter a validar. La validación del texto utilizando el sistema propuesto permitió obtener una tasa de error promedio del: 6.54%, 3.97% y 2.53% al utilizar tres, cinco y siete secuencias, respectivamente. Esta validación corresponde al número de etiquetas que el sistema tiene que verificar para determinar si hay un error en la impresión o no, en el proceso de etiquetado.

Como trabajo futuro se sugiere la implementación del algoritmo y realizar las optimizaciones necesarias para poderlo utilizar en un SBC (en inglés, single board computer), buscando implementar el prototipo en planta, sin la necesidad de requerir un equipo de cómputo de escritorio. La paralelización de las etapas permitiría utilizar el sistema de detección y reconocimiento de texto impreso en líneas de alta velocidad. Otra recomendación para realizar trabajo futuro es diseñar una interfaz gráfica que permita mostrar información detallada sobre el reconocimiento y la detección del texto, presentando la información en un reporte digital y un explorador o visualizador de las imágenes con problemas. También se sugiere como trabajo futuro diseñar un algoritmo que integre la etapa de pre procesamiento y de OCR utilizando otras técnicas de visión, por ejemplo: operaciones morfológicas, umbralización adaptativa; técnicas de machine learning: entrenamiento de clasificadores en cascada, clasificadores SVM, arboles de decisiones; sin dejar de lado también la posibilidad de utilizar técnicas de aprendizaje profundo o transferencia de aprendizaje, aplicado para el caso en específico de la detección de texto en conductores eléctricos.

VII. REFERENCIAS

[1] SAMPSISTEMI, "Cable Extrusion," [Online]. Available: https:// www.sampsistemi.com/cable-extrusion/ [accessed Oct. 20, 2020].

[2] "Wire and cable marking machines." [Online]. Available: https://www.schleuniger.com/en-us/ products/peripherals/marking-/-printing-/-labeling/ [accessed Oct. 20, 2020].

[3] "Coding & Marking Printers | Gem Gravure." [Online]. Available: https://www.gemgravure.com/ coding-marking-printers/ [accessed Oct. 20, 2020].

[4] "Impresoras para tubos y cables | Videojet México." [Online]. Available: https://www.videojet.mx/mx/ homepage/industry-solutions/wire-cablepipe.html [accessed Oct. 20, 2020].

[5] A. K. Bhunia, G. Kumar, P. P. Roy, R. Balasubramanian, and U. Pal, "Text recognition in scene image and video frame using Color Channel selection," Multimed. Tools Appl., vol. 77, no. 7, pp. 8551–8578, Apr. 2018, doi: 10.1007/s11042-017-4750-6.

[6] S. M. Lucas, A. Panaretos, L. Sosa, A. Tang, S. Wong, and R. Young, "ICDAR 2003 robust reading competitions," in Seventh International Conference on Document Analysis and Recognition, 2003. Proceedings., Aug. 2003, pp. 682–687, doi: 10.1109/ICDAR.2003.1227749.

[7] N. V. Rao et al., "Optical character recognition technique algorithms," vol. 16, no. 2, pp. 275-282, 2016.

[8] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," in Advances in Cryptology — EUROCRYPT, pp. 294–311, 2003.

[9] J. B. Pedersen, K. Nasrollahi, and T. B. Moeslund, "Quality inspection of printed texts," in 2016 International Conference on Systems, Signals and Image Processing (IWSSIP), Bratislava, Slovakia, May 2016, pp. 1–4, doi: 10.1109/IWSSIP.2016.7502718.

[10] F. De Sousa Ribeiro et al., "An End-to-End Deep Neural Architecture for Optical Character Verification and Recognition in Retail Food Packaging," in 2018 25th IEEE International Conference on Image Processing (ICIP), Athens, Oct. 2018, pp. 2376–2380, doi: 10.1109/ICIP.2018.8451555.

[11] E. Shelhamer, J. Long, and T. Darrell, "Fully Convolutional Networks for Semantic Segmentation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 4, pp. 640–651, Apr. 2017, doi: 10.1109/TPAMI.2016.2572683.

[12] D. Chen, J.-M. Odobez, and H. Bourlard, "Text detection and recognition in images and video frames," Pattern Recognit., vol. 37, no. 3, pp. 595–608, Mar. 2004, doi: 10.1016/j.patcog.2003.06.001.

[13] K. Messer, J. Kittler, and W. Christmas, "Automatic Sports Classification," in Pattern Recognition, International Conference on, Los Alamitos, CA, USA, Aug. 2002, vol. 2, pp.1005-1008, doi: 10.1109/ ICPR.2002.1048475.

[14] J. C. Rodríguez-Rodríguez, A. Quesada-Arencibia, R. Moreno-Díaz, and C. R. García, "A Character Segmentation Proposal for High-Speed Visual Monitoring of Expiration Codes on Beverage Cans," Sensors, vol. 16, no. 4, Apr. 2016, doi: 10.3390/s16040527.

[15] W. Q. Khan and R. Q. Khan, "Urdu optical character recognition technique using point feature matching; a generic approach," in 2015 International Conference on Information and Communication Technologies (ICICT), Dec. 2015, pp. 1–7, doi: 10.1109/ICICT.2015.7469576.

[16] M. A. H. Monil, M. S. Q. Z. Nine, B. Poon, M. A. Amini, and H. Yan, "Bangla text processing and recognition based on Fuzzy unsupervised Feature Extraction and SVM," in 2013 International Conference on Machine Learning and Cybernetics, Jul. 2013, vol. 03, pp. 1272–1278, doi: 10.1109/ICMLC.2013.6890784.

[17] T. Hassan and H. A. Khan, "Handwritten Bangla numeral recognition using Local Binary Pattern," in 2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), May 2015, pp. 1–4, doi: 10.1109/ICEEICT.2015.7307371.

[18] N. Das, R. Sarkar, S. Basu, M. Kundu, M. Nasipuri, and D. K. Basu, "A Genetic Algorithm Based Region Sampling for Selection of Local Features in Handwritten Digit Recognition Application," Appl Soft Comput, vol. 12, no. 5, pp. 1592–1606, May 2012, doi: 10.1016/j.asoc.2011.11.030.

[19] S. Pasha and M. C. Padma, "Handwritten Kannada character recognition using wavelet transform and structural features," in 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Dec. 2015, pp. 346–351, doi: 10.1109/ERECT.2015.7499039.

[20] C. Liyanage, T. Nadungodage, and R. Weerasinghe, "Developing a commercial grade Tamil OCR for recognizing font and size independent text," in 2015 Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer), Aug. 2015, pp. 130–134, doi: 10.1109/ICTER.2015.7377678.

[21] A. Singh and S. Desai, "Optical character recognition using template matching and back propagation algorithm," in 2016 International Conference on Inventive Computation Technologies (ICICT), Aug. 2016, vol. 3, pp. 1–6, doi: 10.1109/INVENTIVE.2016.7830161.

[22] GitHub, "tesseract-ocr/tesseract," [Online]. Available: https:// github.com/tesseract-ocr/tesseract [accessed Oct. 20, 2020].

[23] G. Van Rossum and F. L. Drake, Python 3 Reference Manual. Scotts Valley, CA: CreateSpace, 2009.

[24] G. Bradski, "The OpenCV Library," Dr Dobbs J. Softw. Tools, 2000.

[25] "OpenCV: Color conversions," [Online]. Available: https://docs. opencv.org/3.4/de/d25/imgproc_color_ conversions.html#color_convert_rgb_lab [accessed Oct. 20, 2020].

[26] S. Raschka and V. Mirjalili, Python machine learning: machine learning and deep learning with Python, scikit-learn, and TensorFlow, Second edition, Fourth release, [fully revised and Updated]. Birmingham Mumbai: Packt Publishing, 04.

[27] A. Kaehler and G. R. Bradski, Learning OpenCV 3: computer vision in C++ with the OpenCV library, First edition, Second release. Sebastopol, CA: O'Reilly Media, 2017.

[28] "Improving the quality of the output," tessdoc. https://tesseract-ocr.github.io/tessdoc/ImproveQuality.html (accessed Oct. 20, 2020).

[29] N. Otsu, "A Threshold Selection Method from Gray-Level Histograms," IEEE Trans. Syst. Man Cybern., vol. 9, no. 1, pp. 62–66, Jan. 1979, doi: 10.1109/TSMC.1979.4310076.

ISSN: 1390 -9266 – 2020 LAJC

AUTHORS

Juan J. Navarro

Es ingeniero de proyectos de automatización en Continuous Improvement Managament Associates S. C. Obtuvo su título de Ingeniero en Mecatrónica en 2012 en la Universidad Autónoma de San Luis Potosí (UASLP), San Luis Potosí, México. Actualmente se encuentra estudiando la Maestría en Manufactura Avanzada en CIATEQ A. C. en el campus San Luis Potosí, México. Sus áreas de interés personales son la visión por computadora y las redes neuronales enfocadas a distintas aplicaciones industriales.

Carolina Reta

Es catedrática CONACYT en CIATEQ A. C. Hidalgo, México, en el departamento de TI, Electrónica y Control, y es miembro del Sistema Nacional de Investigadores Nivel 1 en México. Obtuvo la maestría y el doctorado en Ciencias Computacionales en 2009 y 2014, respectivamente, por el Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), Puebla, México. Sus áreas de investigación son visión por computadora, realidad aumentada, minería de datos e inteligencia artificial. Su investigación se centra en el desarrollo de métodos computacionales innovadores para los campos de la medicina y la ingeniería de manufactura.

ISSN: 1390 -9266 – 2020 LAJC

J. Navarro and C. Reta, "Procesamiento digital de imágenes en la creación de prototipo de sistema inteligente para detección y reconocimiento de texto en etiquetas de conductores eléctricos recubiertos", Latin-American Journal of Computing (LAJC), vol. 7, no. 2, 2020.

Registrador de datos pliviométricos basados en el microcontrolador ATMEL y el transceptor LoRa

Rain gauge data logger based on ATMEL microcontroller and LoRa transceiver

ARTICLE HISTORY

Received 30 September 2020
Accepted 16 October 2020

Kevin Piedra Orellana
DEET
Universidad de Cuenca
Cuenca, Ecuador
kevin.piedra@ucuenca.edu.ec

Fabián Astudillo Salinas
DEET
Universidad de Cuenca
Cuenca, Ecuador
fabian.astudillos@ucuenca.edu.ec

Geovany Lupercio Novillo
DEET
Universidad de Cuenca
Cuenca, Ecuador
geovany.lupercio@ucuenca.edu.ec

Andrés Vázquez Rodas
DEET
Universidad de Cuenca
Cuenca, Ecuador
andres.vazquezr@ucuenca.edu.ec

Ismael Minchala Ávila
DEET
Universidad de Cuenca
Cuenca, Ecuador
ismael.minchala@ucuenca.edu.ec

Registrador de datos pluviométricos basado en el microcontrolador ATMEL y el transceptor LoRa

Rain gauge data logger based on ATMEL microcontroller and LoRa transceiver

Kevin Piedra Orellana
DEET
Universidad de Cuenca
Cuenca, Ecuador
kevin.piedra@ucuenca.edu.ec

Fabián Astudillo Salinas
DEET
Universidad de Cuenca
Cuenca, Ecuador
fabian.astudillos@ucuenca.edu.ec

Geovany Lupercio Novillo
DEET
Universidad de Cuenca
Cuenca, Ecuador
geovany.lupercio@ucuenca.edu.ec

Andres Vázquez Rodas
DEET
Universidad de Cuenca
Cuenca, Ecuador
andres.vazquezr@ucuenca.edu.ec

Ismael Minchala Ávila
DEET
Universidad de Cuenca
Cuenca, Ecuador
ismael.minchala@ucuenca.edu.ec

Abstract — The water and soil program (PROMAS) of the University of Cuenca contributes to the sustainable management of water and soil resources. To carry out this task, PROMAS requires, among others, to monitor environmental parameters using meteorological stations. In the present work, a rainfall data logger was developed on a compact printed circuit board (PCB) using surface mount components. LoRaWAN/ LoRa technology is used to transmit the information. LoRa is one of the LPWAN low power, long range network technologies. LoRaWAN is a protocol that manages end-to-end communication. This development integrates the acquisition, storage and transmission of data. The architecture is made up of a gateway device, the network server, and sensor nodes distributed over the area of interest. The data logger has the additional function of downloading data on-site using WiFi technology. The tests carried out showed that the developed prototype worked correctly in the acquisition, transmission and storage of data.

Keywords — Pluviometer; LoRaWAN; LoRa; gateway; WiFi.

Resumen — *El programa del agua y el suelo (PROMAS) de la Universidad de Cuenca contribuye al manejo sostenible de los recursos agua y suelo. Para llevar a cabo este cometido, el PROMAS requiere, entre otros, monitorear parámetros ambientales utilizando estaciones meteorológicas. En el presente trabajo se desarrolló un registrador de datos pluviométricos en un PCB compacto utilizando componentes de montaje superficial. Para transmitir la información se usa la tecnología LoRaWAN/LoRa. LoRa es una de las tecnologías de redes de largo alcance y bajo consumo LPWAN. LoRaWAN es un protocolo que gestiona la comunicación de extremo a extremo. Este desarrollo integra la adquisición, el almacenamiento y la transmisión de los datos. La arquitectura está integrada por nodos sensores distribuidos en toda el área de interés, un dispositivo gateway y el servidor de red. El registrador de datos tiene como función adicional la descarga de datos in-situ usando tecnología WiFi, para esto se utiliza un gateway. Las pruebas realizadas mostraron que el prototipo desarrollado funcionó correctamente en la adquisición, transmisión y almacenamiento de datos.*

Palabras clave — *Pluviómetro; LoRaWAN; LoRa; gateway; WiFi.*

ISSN: 1390 -9266 – 2020 LAJC

I. INTRODUCCIÓN

El PROMAS es un departamento de investigación de la Universidad de Cuenca. Este departamento tiene como misión contribuir al "manejo sostenible de los recursos agua y suelo, mediante la generación de conocimiento científico, la capacitación y la extensión; aplicando nuevas tecnologías y adaptando metodologías que permitan dar soluciones integrales, en equilibrio ambiental y con responsabilidad social". Para cumplir con este cometido, el PROMAS requiere, entre otros, monitorear ciertos parámetros ambientales utilizando estaciones meteorológicas (alrededor de 130) distribuidas en un área geográficamente extensa. El área de interés comprende desde el sector del Cajas en la provincia del Azuay y se extiende hasta la provincia del Cañar. Las estaciones miden varios parámetros hidro-meteorológicos, entre ellos la cantidad de lluvia. Las mediciones son usadas con fines de investigación en diferentes proyectos [1].

Las estaciones cuentan con un registrador de datos. El registrador realiza la adquisición de los parámetros hidro-meteorológicos y los almacena localmente. Los datos pluviométricos brindarán la posibilidad de disponer de información para evaluar crecidas, calcular balances de agua de los ríos, etc. Los datos recolectados por los registradores requieren ser transmitidos/copiados a los servidores del PROMAS ubicados en el campus central de la Universidad de Cuenca [1].

Actualmente, para la mayoría de las estaciones hidro-meteorológicas, la recolección de datos se la realiza in-situ. El personal del PROMAS se desplaza a dichas estaciones para copiar los datos almacenados en cada una de ellas. En general, la periodicidad de visita a las estaciones es de entre 30 a 45 días. El acceso a estas estaciones resulta complicado debido a que están distribuidas en un área geográficamente extensa y una buena parte de ellas en lugares de difícil acceso [1].

Con estos antecedentes, en el presente trabajo se propone el diseño e implementación de un dispositivo registrador de datos pluviométricos con capacidad de comunicación LoRa y LoRaWAN, utilizando componentes de montaje superficial. El transceptor usado en la implementación es el módulo LoRa SX1278. El diseño del dispositivo contempla minimizar el tamaño del PCB, reducir el consumo energético, transmitir a largo alcance (al menos 1 Km [2]) en quasi-tiempo real (cada 5 minutos según el requerimiento del PROMAS). Adicionalmente, el dispositivo dispone de una función de descarga de datos in-situ a través de la tecnología WiFi.

El resto de este documento está organizado de la siguiente manera. La Sección II describe los trabajos relacionados. Por otro lado, en la Sección III se presenta la metodología aplicada. La Sección IV presenta el diseño e implementación del sistema. La Sección V expone los resultados de la evaluación del prototipo. La Sección VI presenta las conclusiones. Finalmente, la Sección VII resume los trabajos futuros.

II. TRABAJOS RELACIONADOS

El protocolo y arquitectura LoRaWAN es aplicado a varias soluciones en las que se requiere la transmisión remota de datos a largo alcance y con un bajo consumo energético. Por ejemplo, en [3] se realiza la comparación de dos soluciones (WM Bus y LoRaWAN) para la conectividad de medidores inteligentes con respecto a la duración de las baterías. En el estudio se muestra que los medidores que usan LoRaWAN tienen un tiempo de servicio mucho más largo que los medidores que usan WM Bus. En [4] se muestra la implementación de una red inalámbrica de sensores (WSN) LoRaWAN diseñada para aplicaciones de monitoreo de salud estructural en el campo de la construcción. En [5], se usa LoRaWAN para la recopilación constante de datos de colonias de abejas. Los datos recopilados se transmiten a un centro de datos remoto para su posterior análisis. En el estudio [6], se usa el protocolo LoRaWAN para la transmisión de datos de salud en sistemas de atención médica o datos críticos de salud en entornos de desastre.

Por otro lado, existen varias propuestas de diseño de registradores de adquisición y transmisión de datos meteorológicos basados en microcontroladores y transceptores de bajo consumo energético [7], [8]. Las tecnologías usadas en estos trabajos fueron LoRa y Zigbee. Estos dispositivos desarrollados cuentan con la capacidad de recopilar, almacenar y transmitir la información con un área de cobertura de largo alcance. En las pruebas de alcance se observó la superioridad del uso de dispositivos con tecnología LoRa con respecto a las demás

tecnologías. Además, se desarrolló un sistema de registro de datos sobre la cantidad de lluvia utilizando la placa LoPy4 [9].

En el presente trabajo se busca reducir el costo, el consumo de energía del registrador de datos pluviométricos, pero sobre todo la innovación radica en que los datos adquiridos son transmitidos inalámbricamente al servidor del PROMAS, por lo tanto, ya no se necesita hacer visitas in-situ. Para lo cual, en el diseño se utiliza un microcontrolador Atmel (ATMega 1284p) y el módulo transceptor LoRa SX1278. Además, se implementa el protocolo LoRaWAN en el microcontrolador Atmel en base a la implementación Arduino-LMIC library [10].

III. MÉTODO

El consumo de energía de los sistemas embebidos depende de los componentes que son incluidos en el diseño del prototipo para su desarrollo. Por lo tanto, se requiere tener el conocimiento de las características técnicas y principales sobre el consumo energético de algunos microcontroladores, previo al diseño del registrador de datos pluviométricos.

En la Tabla I se presenta un resumen de las características más relevantes de los microcontroladores seleccionados que cumplieron con los requisitos que se necesita en este prototipo, entre ellos el uso de memoria programable, compatibilidad con los dispositivos LoRa, el bajo costo y consumo de energía.

TABLA I. COMPARATIVA DE LOS MICROCONTROLADORES SELECCIONADOS [7]

Microcontroladores	*Voltaje de Operación (V)*	*Temperatura (°C)*	*Modo Activo (A)*	*Modo de Ahorro de Energía (A)*
STM32L053R8	1.65 a 3.6	-40 a 125	88 µ	0.8 µ
ATmega 328p	1.8 a 5.5	-40 a 85	0.3 m	0.8 µ
Atmega 1284p	1.8 a 5.5	-40 a 85	0.3 m	0.6 µ
MSP-EXP432P401R	3.3 a 5	-40 a 85	80 µ	660 n
PIC32MX340F512H	7 a 15	-40 a 125	75 m	0.9 m

Tras el análisis de las características técnicas de los microcontroladores, se consideró como la mejor opción el uso del microcontrolador ATmega1284p por la compatibilidad con los sensores y demás dispositivos utilizados, su facilidad de implementación con el transceptor LoRa, además de tener mayor capacidad en la memoria de programa y menor costo que los otros componentes.

Una vez seleccionado el microcontrolador, se procede a seleccionar el transceptor LoRa. En [7] se realizó la implementación del circuito RF del transceptor LoRa usando los servicios de construcción y ensamblaje de PCBs disponibles localmente, con el fin de abaratar los costos en el producto final, sin embargo, se tuvieron varios problemas a la hora de implementarlo. En nuestro medio no hay empresas que provean servicios de soldado de componentes de montaje superficial automático. El montaje de los componentes fue a mano y se produjeron varias imprecisiones a la hora de soldarlos, como por ejemplo en la unión de dos pines por una pequeña cantidad de suelda.

En consecuencia, se buscaron dispositivos LoRa con los componentes RF integrados, para el diseño se decidió usar específicamente el Ra02 LoRa SX1278. Este viene encapsulado para montaje superficial y directamente con un pin de conexión RF para la antena. Entre sus características están: bajo consumo energético, frecuencia y corriente configurable. La frecuencia de operación es de 433 MHz. Su sensibilidad es mayor a -148 dBm y contiene un amplificador de potencia de +20 dBm. El voltaje de alimentación es de 1.8 a 3.7 V. La corriente en modo recepción para los módulos SX1278 es de 9.9 mA. La corriente en modo transmisión puede ser configurada desde 10 mA a 240 mA, siendo 100 mA la corriente sugerida por el fabricante [11]. Luego del análisis de componentes se procedió a hacer un trabajo de reingeniería del trabajo [9].

IV. DISEÑO E IMPLEMENTACIÓN

La Figura 1 muestra el diagrama de bloques del prototipo de registrador de datos pluviométricos propuesto. El sistema requiere un bajo consumo de energía, un alcance de al menos 1 km, la adquisición de la señal del sensor pluviométrico, el almacenamiento, y la transmisión en quasi-tiempo real. Adicionalmente, se requiere que el dispositivo transmita información sobre el estado del equipo usando los parámetros de temperatura, humedad, y nivel de carga de la batería, junto con información temporal de fecha y hora.

ISSN: 1390 -9266 – 2020 LAJC

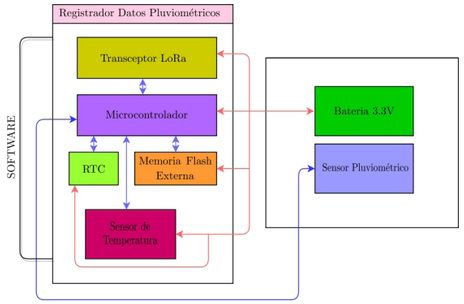


Fig. 1. Diagrama de bloques del diseño del prototipo.

El dispositivo es desarrollado para cumplir las funciones de medición, transmisión y almacenamiento de varias variables en determinados intervalos de tiempo. Para el diseño se utilizó un transceptor con tecnología LoRa, un microcontrolador de bajo consumo de energía, una memoria flash, un sensor de temperatura y humedad, un reloj de tiempo real (RTC, Real Time Clock) y un sensor pluviométrico.

A. Esquemático del dispositivo

La Figura 2 presenta el diagrama de bloques de la estación pluviométrica. Inicialmente, en el diagrama se encuentra el módulo transceptor LoRa SX1278 Ra-02 (bloque 1), que es el encargado de la transmisión hacia la antena RF. En el bloque 2 se ubica el microcontrolador ATMega 1284p, su función es el control del sistema y de la comunicación con los dispositivos, en este caso con la memoria flash externa (bloque 3), el RTC (bloque 4), transceptor LoRa (bloque 1) y los sensores (bloque 5). Por último, para futuras expansiones con nuevos sensores o dispositivos, se añadieron pines de control analógicos/digitales (bloque 6).

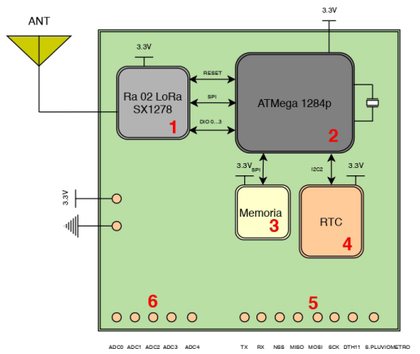
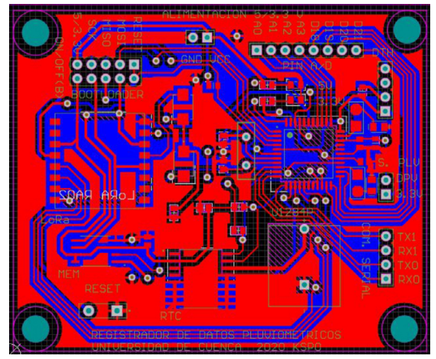


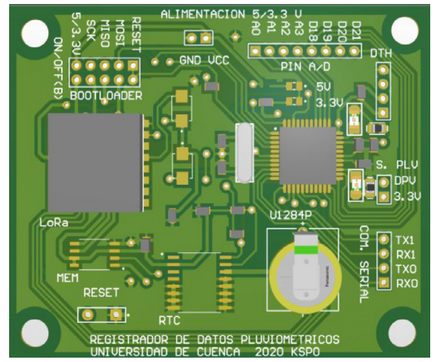
Fig. 2. Diagrama de bloques de la estación pluviométrica.

B. Características del PCB

Las dimensiones del PCB desarrollado son de 75.86 × 63.294 mm. Las pistas de conexión tienen un grosor de 0.35 mm y las de alimentación de 0.5 mm. Como regla de diseño cuenta con un clearance de 0.25 mm para evitar un acople indeseado (crosstalk), debido a la cercanía de las pistas. Los componentes se agrupan según las señales a procesar, esto se hace para reducir la distancia de las pistas y los efectos parásitos resistivos e inductivos. Los componentes usados son de montaje superficial. En las Figuras 3a y 3b se muestra el diseño PCB del prototipo final en 2D y 3D respectivamente. En el modelo 2D se encuentran visibles todas las capas disponibles, mientras que en el modelo 3D se muestra el diseño PCB, en el cual fue añadido el screen laminado para la identificación de los pines de comunicación, alimentación y control.



(a) PCB en 2D



(b) PCB en 3D

Fig. 3. Diseño final del PCB del dispositivo (a). 2D. (b). 3D.

C. Protocolo LoRaWAN

El protocolo LoRaWAN es una especificación para redes de baja potencia y área amplia (LPWAN, Low Power Wide Area Network). Este protocolo es también usado para la especificación de la arquitectura de red del sistema. La capa física de LoRaWAN es Long Range (LoRa), esta habilita el enlace físico de comunicación. Las ventajas de usar LoRaWAN son: una comunicación de largo alcance, un menor consumo de energía, y su bajo costo (infraestructura mínima, nodos finales de bajo costo, software abierto).

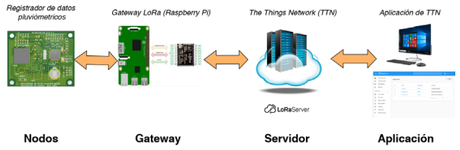


Fig. 4. Arquitectura de la red LoRaWAN.

La arquitectura de red LoRaWAN consta de nodos sensores (dispositivos finales), gateways (puertas de enlace), un servidor de red y servidores de aplicaciones (Figura 4). En una red LoRaWAN, un nodo sensor adquiere los datos meteorológicos, que son transmitidos y recibidos por múltiples gateways. Cada gateway reenviará el paquete recibido al servidor de red a través de la red celular, Ethernet, WiFi o satélite. El software que se ejecuta en el gateway es responsable de reenviar cualquier paquete de datos entrantes al servidor de red. A su vez, el servidor de red envía y recibe mensajes LoRaWAN hacia y desde dispositivos, que se comunican con servidores de aplicaciones ascendentes. El servidor de aplicaciones es el destino final de los datos de la aplicación del dispositivo, enviados como carga útil (payload) en los mensajes de LoRaWAN [11].

a) Nodo final LoRa

Los nodos finales, que pueden estar físicamente fijos o móviles, transmiten datos del sensor a un gateway LoRa. Se puede construir un nodo final combinando varias opciones de *hardware y software*. La Figura 3 muestra la implementación del prototipo PCB del nodo final.

Para la configuración de la red LoRaWAN se seleccionó el método de activación por personalización (ABP). El uso de este método requiere definir los siguientes valores:

- Dirección del nodo *(DevAddr)*.
- Clave de sección de aplicación *(AppSKey)*.
- Clave de sección de red *(NwkSKey)*.

Los valores *DevAddr, AppSKey y NwkSKey* se configuran en el microcontrolador ATMega 1284p y en el servidor LoRa para el proceso de autenticación. Para inicializar el nodo en modo LoRaWAN se definen la dirección, las claves, el tipo de activación, y la frecuencia en la que opera el transceptor LoRa, en este caso 433 MHz.

b) LoRa Gateway

Los *gateways* LoRaWAN deben tener mayor capacidad de procesamiento que los nodos finales. Por esta razón, se procedió a implementar un gateway LoRa con un Raspberry Pi. El gateway LoRa consta de un transceptor de radio, un microprocesador, una fuente de alimentación y una antena. El Raspberry Pi funciona como un reenviador de paquetes. Toda la comunicación entre el transceptor de radio LoRa y el Raspberry Pi se manejará usando comunicación serial SPI (Figura 5).

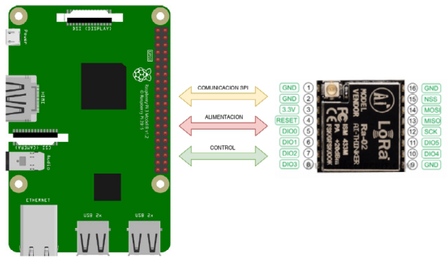


Fig. 5. Gateway LoRaWAN basado en Raspberry Pi y el módulo LoRa Ra02 SX1278.

c) The Things Network

The Things Network (TTN) desarrolla una implementación de un servidor de red mundial LoRaWAN. Esta red permite conectar los gateways, registrar dispositivos y enviar/recibir datos en quasi-tiempo real. La ventaja de TTN es que se puede usar de manera gratuita. En la Figura 6 se observa el interfaz de la consola de TTN, que tiene disponible las aplicaciones y los gateways que se requieran registrar.

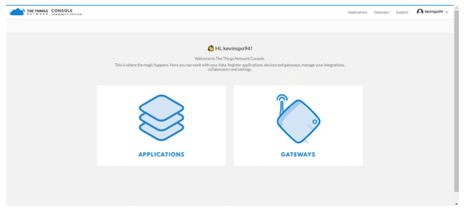


Fig. 6. Interfaz de la consola de TTN.

ISSN: 1390 -9266 – 2020 LAJC

Para la visualización de los datos de las aplicaciones en TTN, las cargas útiles tienen que ser decodificadas. En la aplicación, TTN tiene una sección para desarrollar el decodificador en el lenguaje Javascript. Para este caso, esto permite reconocer si los paquetes de datos son del sensor pluviométrico o del estado del dispositivo.

D. Almacenamiento de datos

La información del dispositivo se almacena en dos tipos de archivos: de configuración y de datos. El archivo de configuración rain.cnf, contiene la información de configuración de la estación. En este archivo se escribe el intervalo de tiempo de cada periodo en el que los datos se van a almacenar en memoria y enviar hacia el servidor. Además, la configuración de las credenciales del enlace ABP entre el nodo y la aplicación del servidor.

Para el almacenamiento de los datos recolectados por el dispositivo, se crean dos grupos de archivos. El primer archivo almacena datos del sensor de lluvia, su prefijo es *(sensor-[fecha].dat)*. El segundo archivo almacena información de estado sobre el nivel de batería, temperatura y humedad del ambiente en el que se encuentra el nodo; su prefijo es (estado-[fecha].dat). Los registros del sensor se almacenan de manera predeterminada cada 5 minutos, o en función del periodo configurado en el archivo *rain.cnf*. El estado se almacena cada 60 minutos. Estos tiempos de almacenamiento son definidos en base a los requerimientos del PROMAS. A continuación, se detalla la estructura de cada uno de los archivos.

a) Estructura del archivo para almacenamiento de datos

Se definen dos tipos de registros: registro de datos (Figura 7) y registro de estado (Figura 8). El registro de datos tiene la información adquirida por el sensor de lluvia; estos datos se almacenan por defecto cada 5 minutos, el tamaño de cada registro es de 64 bits. Por su parte, el registro de estado almacena información sobre la condición interna del registrador de datos. La información de estado se almacena cada hora y el tamaño de cada registro es de 72 bits.

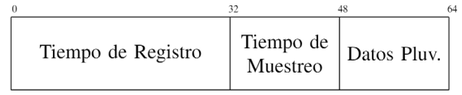


Fig. 7. Estructura de trama para el almacenamiento en el archivo del sensor de lluvia.

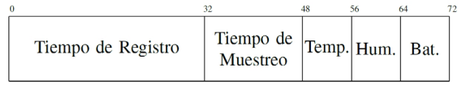


Fig. 8. Estructura de trama de datos para el almacenamiento en el archivo de estado.

V. RESULTADOS

En esta sección se describen los resultados obtenidos durante el diseño, construcción y pruebas del prototipo. Se detalla el funcionamiento final y los resultados obtenidos en varias evaluaciones relacionadas con el almacenamiento, la transmisión, y el consumo energético del sistema.

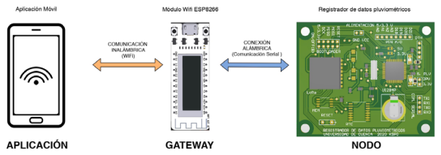


Fig. 9. Arquitectura de la red para la descarga de datos in-situ.

A. Descarga de datos in-situ

Para la descarga de datos intervienen tres dispositivos: un nodo sensor, un gateway in-situ y un dispositivo móvil (Figura 9). El gateway se conecta a los nodos sensores utilizando comunicación serial UART. Para la comunicación entre el dispositivo móvil y el gateway in-situ se usa WiFi.

B. Nodo

El nodo, es decir, el registrador de datos (Figura 3), es el encargado de responder las solicitudes enviadas desde la aplicación móvil por medio del *gateway* in-situ. La conexión entre el nodo y el gateway in-situ se realiza de manera alámbrica. El *gateway* dispone de un

cable ethernet conectado internamente, este se conecta al puerto de red RJ45 con protección IP67 integrado en el nodo. Para la comunicación entre el nodo y el gateway in-situ se usa UART.

C. Gateway in-situ

El módulo que va a actuar como gateway in-situ es el Wifi Kit 8. Este es un módulo ESP8266 (Figura 10), que incluye un sistema de administración de batería Li-Po y una pantalla OLED de 0.9. Para establecer la comunicación entre el nodo y el dispositivo móvil, se desarrolló el software que permite procesar las peticiones realizadas y el reenvío de los paquetes hacia la aplicación móvil, mediante el protocolo HTTP.

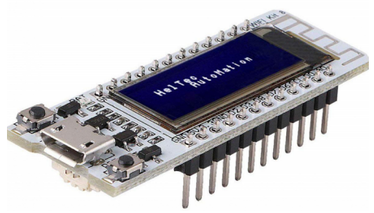


Fig. 10. Módulo Wifi Kit 8

El módulo WiFi es alimentado con una batería Li-Po de 3.7 V, además se integra un cable Ethernet para tener acceso al nodo. Para unirse a la red inalámbrica, se configura el nombre y la contraseña, que son ingresados desde el dispositivo móvil.

D. Aplicación Móvilt

Con el objetivo de visualizar y decodificar los datos adquiridos y almacenados por el nodo, se implementó una aplicación móvil. La aplicación es nativa para dispositivos con sistema operativo Android, y fue desarrollada en el lenguaje JAVA. La aplicación móvil, permite al usuario buscar los archivos almacenados en memoria (Sección D), mediante dos campos de búsqueda: fecha y tipo de archivo. Si el archivo existe, se visualizan los datos en pantalla. Además se dispone de la función para la descarga del archivo en formato *(.csv)*. El interfaz de la aplicación móvil se muestra en la Figura 11.

Fig. 11. Interfaz de la aplicación móvil.

Adicionalmente, la aplicación tiene la opción de configuración de parámetros, la cual permite cambiar los intervalos de tiempo de cada registro, así como las credenciales de autenticación de ABP de la aplicación del servidor LoRaWAN.

E. PCB

El diseño presentado en la Sección B se envió a la manufactura en una empresa local especializada. En la Figura 12 se muestra la vista superior del PCB con los componentes soldados, en tanto que en la Figura 13 se muestra la vista inferior.

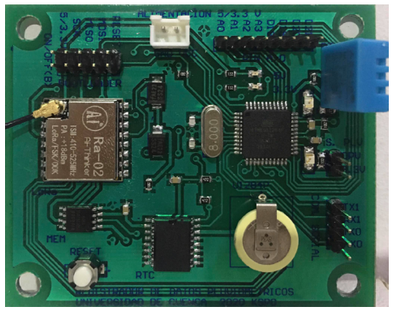


Fig. 12. Aspecto final del PCB con componentes de montaje superficial (vista superior)

ISSN: 1390 -9266 – 2020 LAJC

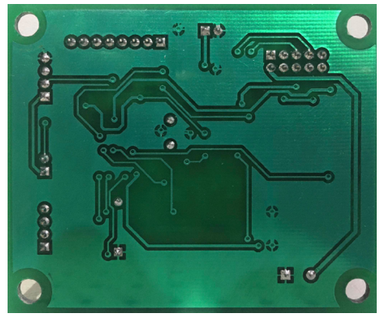


Fig. 13. Aspecto final del PCB con componentes de montaje superficial (vista inferior).

F. Pruebas de laboratorio

a) Transmisión

Para la transmisión de datos hacia el servidor LoRaWAN se utilizaron los dispositivos: nodo, *gateway* LoRa y un ordenador (detallados en la Sección C). El nodo transmite los datos hacia al *gateway* LoRa y este reenvía los paquetes hacia el servidor TTN. Los paquetes del sensor son recibidos cada 5 minutos y los datos del estado del nodo cada 60 minutos. Los datos en recepción son visualizados en la aplicación del servidor LoRaWAN de TTN (Figura 14).

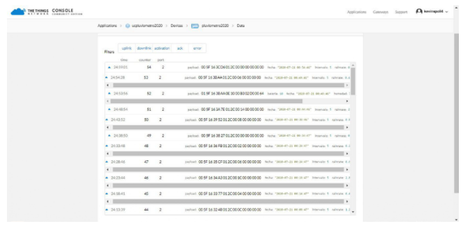


Fig. 14. Visualización de datos en la aplicación del servidor TTN.

El detalle de un paquete con información recolectada por un sensor se muestra en la Figura 15, y la información del estado del nodo se muestra en la Figura 16. En el paquete del sensor se muestran: la fecha, el intervalo de transmisión y la cantidad de lluvia. En el paquete del estado se encuentran los datos de la batería, la fecha y hora, la temperatura y humedad, y el intervalo de transmisión de cada paquete. Adicionalmente, todos los paquetes tienen metadatos con información de la conexión LoRaWAN como: la frecuencia, *data rate* (DR), *coding rate* (CR), *signal-to-noise ratio* (SNR), *received signal strength indicator* (RSSI) y el tiempo en el que llegó el paquete.

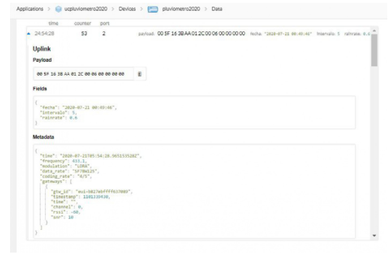


Fig. 15. Visualización de datos recolectados por el sensor en la aplicación del servidor TTN.

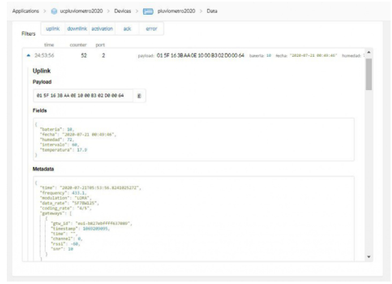
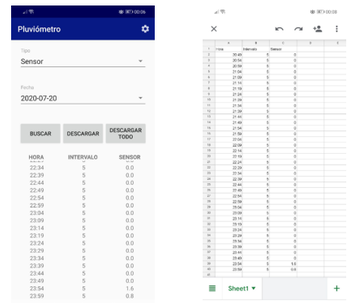


Fig. 16. Visualización de datos del estado del dispositivo en la aplicación del servidor TTN.

b) Descarga de datos in-situ

Para descargar los datos guardados en el nodo sensor, se desarrolló una aplicación móvil. Los nombres de los archivos almacenados en el nodo corresponden a la fecha de registro de datos. Cada archivo contiene las muestras registradas del sensor pluviométrico y del estado del dispositivo. La aplicación permite descargar los datos en el dispositivo móvil en formato *(.csv)*. En las Figuras 17a y 17b se muestra un ejemplo de los datos del sensor pluviométrico visualizados en la aplicación móvil y descargados en formato *(.csv)*.



(a) *(b)*

Fig. 17. Visualización de datos del sensor: (a) Datos en la aplicación móvil, (b) Datos almacenados en el dispositivo móvil en un archivo (.csv)

Teniendo un registro de la información con la tasa de muestreo designada a cada paquete: de sensor 5 minutos y de estado del dispositivo 60 minutos (Sección D). Para los datos del sensor se escriben 288 registros diarios de 8 Bytes (2304 Bytes) y para los datos del estado se escriben 24 registros diarios de 9 Bytes (216 Bytes), por lo tanto, el dispositivo escribe 2520 Bytes cada día en la memoria. De esta manera, con la memoria flash de 16 MB de capacidad, y el dispositivo funcionando de forma continua, el periodo de registro de datos es de 16777216 Bytes/2520 Bytes = 6657 días, o 6657/365 = 18.23 años.

c) Configuración de parámetros del dispositivo

La aplicación móvil además de la descarga de datos, tiene la función de configuración de parámetros. Para verificar el funcionamiento se ingresaron los parámetros de tiempo de muestreo de cada uno de los paquetes y las credenciales para enlazarse a la aplicación del servidor TTN. En la Figura 18 se observa cómo se ingresan los nuevos parámetros en la configuración. Por ejemplo, los paquetes de datos del sensor cada minuto y de estado del nodo cada 3 minutos. Además, de las nuevas credenciales DevAddr, NwkSKey y AppSKey. En la Figura 19, se muestran los datos de prueba que llegaron al servidor usando la configuración de ejemplo.

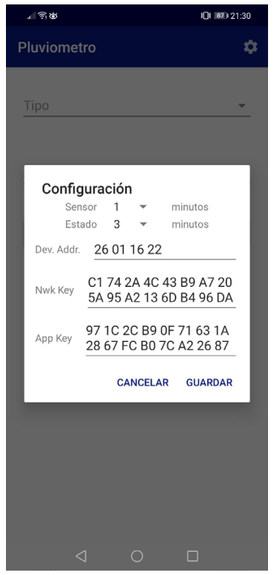


Fig. 18. Ventana de configuración de parámetros del nodo.

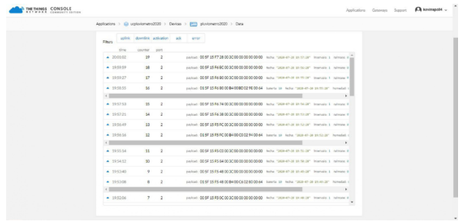


Fig. 19. Verificación de los paquetes de datos en la aplicación del servidor TTN.

G. Pruebas de consumo energético

El dispositivo desarrollado está destinado a funcionar en ubicaciones en las que generalmente no se tiene alimentación desde la red eléctrica, por lo que es importante conocer y optimizar su consumo energético. El voltaje de funcionamiento del nodo es de 3.3 V.

El análisis del consumo se realiza utilizando la metodología propuesta por Nguyen [12]. Los tiempos activos por componente (ciclo de trabajo) se utilizan para calcular el consumo total. El período de tiempo del ciclo de trabajo es de 5 minutos. Este tiempo lo establecen los requisitos de las aplicaciones del PROMAS. Durante este período, la información se transmite al centro de datos.

El análisis energético del registrador de datos contempló tres partes: adquisición y control, el sensor, y la transmisión. El proceso de adquisición del sensor de lluvia y el control de los dispositivos permanece activo todo el tiempo. Por lo tanto, el dispositivo involucrado en este proceso tiene un ciclo de trabajo del 100 %. El consumo del sensor de lluvia es de 0.034 mA para el valor máximo medido. La precipitación máxima en el área geográfica de interés, a partir de los datos registrados por el PROMAS, es de 22 mm en una hora (entre los años 2015 y 2017), con este valor el sensor consumiría 0.088 mA [9].

La transmisión por medio del transceptor LoRa está configurado con un factor de dispersión de 7 y un ancho de banda de 125 kHz. El ciclo de trabajo del transceptor es de 0.062 % si se considera un tiempo de transmisión de 186 ms. La Tabla II presenta el consumo promedio de cada componente del registrador de datos y el consumo general, que es de 28.510 mW.

ISSN: 1390 -9266 – 2020 LAJC

TABLA II. ESTIMACIÓN DEL CONSUMO DE ENERGÍA DEL REGISTRADOR DE DATOS

Dispositivos	*Modo*	*Consumo de Corriente (mA)*	*Ciclo de Trabajo (%)*	*Corriente Promedio (mA)*	*Potencia (mW) (I x 3.3V)*
Adquisición y Control	Activo Reposo	8,624 0,000	100,00 0,00	8,624	28,459
Sensor	Activo Reposo	0,008 0,000	1,29 98,71	0,001	0,003
Transmisión	Activo Reposo	23,896 0,000	0,06 99,94	0,014	0,048
Consumo de energía promedio general					28,510

En las pruebas de laboratorio realizadas, se usó una fuente de alimentación continua regulable (0-20) V, la cual fue configurada a 3.3 V, voltaje requerido para el funcionamiento del registrador de datos. El consumo de corriente fue medido con un amperímetro conectado en serie entre el pin positivo de la fuente y el pin de entrada (Vin) del registrador de datos. En el proyecto de investigación ``Aplicación de tecnologías inalámbricas al sistema de predicción de caudales en la cuenca del río Tomebamba'' se usan baterías de ácido sólido de 7200 mAh-12 V. Por lo que en este proyecto se utilizará el mismo tipo de batería, integrando un controlador de carga a 3.3 V en pruebas de campo. Esta batería contiene una carga mínima del 25 %. Entonces, el tiempo teórico para el próximo ciclo de recarga es 0.75 × 7200$ mAh × 12 V /28.510 mW = 2272.886 horas = 94 días. Este dato es aproximado, puesto que entre la batería y el dispositivo desarrollado hay que usar un convertidor *step-down* que tiene un consumo adicional.

H. Reseña sobre los costos

El PROMAS actualmente envía los dispositivos desarrollados a una empresa local para su manufactura. El microcontrolador y el transceptor del prototipo desarrollado tuvo un costo aproximado de $50, mientras que el dispositivo LoPy4 utilizado en [9] (microcontrolador + transceptor), tiene un costo de $84 en el mercado local, por lo que el prototipo actual tiene una reducción del costo en estos elementos de un 40 %.

VI. CONCLUSIONES

La implementación del protocolo LoRaWAN permitió la transmisión de los datos pluviométricos remotamente en quasi-tiempo real hacia el servidor LoRaWAN The Things Network (TTN). Las pruebas que se realizaron para la transmisión de datos hacia el servidor LoRaWAN fueron satisfactorias. El servidor TTN permitió observar los datos recibidos en su interfaz web.

Los datos pluviométricos fueron adquiridos y descargados correctamente en la aplicación móvil, validando así los requerimientos solicitados por el PROMAS.

Mediante las pruebas de laboratorio realizadas respecto al consumo energético del registrador de datos se verificó que, el consumo es aproximadamente un 50 % menor al de los dispositivos desarrollados en trabajos anteriores. Esto debido a los cambios realizados en la arquitectura del diseño, su funcionamiento a 3.3 V, y la adaptación de todos los componentes para trabajar a este nivel de tensión.

Finalmente, en el desarrollo del prototipo se obtuvo la reducción de costos, en la manufactura, producción y adquisición de componentes. Por lo que, el PROMAS en el desarrollo de este prototipo a gran escala obtendrá un ahorro de costos significativo en comparación a los dispositivos desarrollados en trabajos anteriores.

VII. TRABAJOS FUTUROS

En este proyecto, no se consideró el desarrollo de un controlador de carga, debido a que se tuvo que delimitar el alcance. Por lo que es necesario desarrollar un controlador de carga, para integrar una batería y un panel solar.

El dispositivo fue desarrollado exclusivamente para el PROMAS. Sin embargo, si este puede ser usado por otras instituciones, debido a que un alto porcentaje de usuarios usan dispositivos móviles con sistema operativo iOS, podría ser necesario implementar una aplicación móvil para dichos dispositivos.

VIII. REFERENCIAS

[1] F. Astudillo-Salinas y A. Vazquez-Rodas, «Aplicación de tecnologías inalámbricas al sistema de predicción de caudales en la cuenca del río Tomebamba,» 2016.

[2] S. Daud, T. S. Yang, M. A. Romli, Z. A. Ahmad, N. Mahrom y R. A. A. Raof, «Performance Evaluation of Low Cost LoRa Modules in IoT Applications,» IOP Conference Series: Materials Science and Engineering, vol. 318, p. 012053, 3 2018.

[3] L. Vangelista, L. Dell'Anna y P. Palazzzoli, «A battery lifetime comparison between LoraWAN and Wireless MBus smart meters,» de 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2019.

[4] G. Loubet, A. Takacs, E. Gardner, A. De Luca, F. Udrea y D. Dragomirescu, «LoRaWAN Battery-Free Wireless Sensors Network Designed for Structural Health Monitoring in the Construction Domain,» Sensors, vol. 19, 2019.

[5] A. Zacepins, J. Jelinskis, A. Kviesis, M. Dzenis, V. Komasilovs y O. Komasilova, «Application of LoRaWAN technology in Precision Beekeeping.,» East Sarajevo, Bosnia-Herzegovina, 2018.

[6] M. T. Buyukakkaslar, M. A. Erturk, M. A. Aydin y L. Vollero, «LoRaWAN as an e-Health Communication Technology,» de 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), 2017.

[7] A. C. Lopez Ochoa, «Diseño e implementación de un registrador de datos para la adquisición de información limnigráfica,» 2019.

[8] M. P. Gutama Morocho y J. J. Vazquez Patino, «Prototipo de un dispositivo de adquisición, almacenamiento y transmisión de datos meteorológicos usando los transductores de la estación DAVIS 6162 Wireless Vantage Pro2 Plus,» 2017.

[9] S. Placencia, F. Astudillo-Salinas, A. Vazquez-Rodas, I. Minchala y J. Guaman, «Rainfall Intensity Datalogger System. LoPy4-Based Design and Implementation,» 2019.

[10] M. Kooijman, «Lmic Library».

[11] P. Seneviratne, "Beginning LoRa Radio Networks with Arduino: Build Long Range," Low Power Wireless IoT Networks, pp. 12-18, 2019.

[12] T. Nguyen, «Energy efficient wireless sensor network and low power consumption station design for an urban water level monitoring system,» de 2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS), 2016.

ISSN: 1390 -9266 – 2020 LAJC

AUTHORS

Kevin Piedra Orellana

Recibió el título de tercer nivel en Ingeniería Electrónica y Telecomunicaciones de la Universidad de Cuenca, Cuenca, Ecuador, en 2020. Sus intereses de investigación incluyen codificación de redes, redes de sensores inalámbricos, simulación de redes, rendimiento de redes, ciberseguridad.

Fabián Astudillo Salinas

Recibió el título de tercer nivel en Ingeniería de Sistemas de la Universidad de Cuenca, Cuenca, Ecuador, en 2007, y los grados de MSc. y Ph.D del "Institut National Polytechnique de Toulouse", Toulouse, Francia, en 2009 y 2013, respectivamente. Desde 2013 es Investigador a Tiempo Completo del Departamento de Ingeniería Eléctrica, Electrónica y Telecomunicaciones de la Universidad de Cuenca, Cuenca, Ecuador. Sus intereses de investigación incluyen redes de sensores inalámbricos, redes vehiculares, simulación de redes, ciberseguridad y HPC

Geovany Lupercio Novillo

Estudió Ingeniería Electrónica en la Universidad Politécnica del Litoral en la ciudad de Guayaquil. En el 2008 Obtuvo su Diplomado en Administración y Telecomunicaciones en la Universidad de Guadalajara Jalisco - México y en el 2009 su Maestría en Administración de las Telecomunicaciones en la Universidad de Guayaquil. Sus intereses de investigación son los efectos de las radiaciones no ionizantes, aplicaciones de tecnologías inalámbricas, y aplicaciones de IoT.

Andrés Vázquez Rodas

Recibió el grado de Ingeniero Electrónico en el año 2004 de la Universidad Politécnica Salesiana Cuenca – Ecuador, el grado de master en Telemática (con honores) de la Universidad de Cuenca – Ecuador in 2010, y el grado de Ph.D. del Departamento de Ingeniería Telemática de la Universitat Politècnica de Catalunya BarcelonaTech (UPC), España en 2015. Desde el 2015, es profesor a tiempo completo en la Universidad de Cuenca en el Departamento de Eléctrica, Electrónica y Telecomunicaciones (DEET). Sus intereses de investigación incluyen redes inalámbricas malladas, redes inalámbricas de sensores, redes industriales y sistemas complejos.

ISSN: 1390 -9266 – 2020 LAJC

Ismael Minchala Ávila

Recibió el grado de Ingeniero Electrónico en la Universidad Politécnica Salesiana, Cuenca, Ecuador, en 2006, y los grados de M.Sc. y Ph.D. en Ingeniería de Control del Tecnológico de Monterrey, Monterrey, México, en 2011 y 2014, respectivamente. Obtuvo una beca Postdoctoral en el Tecnológico de Monterrey en el grupo de investigación de cambio climático. Es actualmente investigador a tiempo completo en el Departamento de Ingeniería Eléctrica, Electrónica y Telecomunicaciones en la Universidad de Cuenca, Ecuador. Sus interéses de investigación son control tolerante a fallas aplicados a sistemas de energía, automatización y control de procesos.

LATIN-AMERICAN JOURNAL OF COMPUTING (LAJC), Vol VII, Issue 2, December 2020

Uso de la tecnología en Industria 4.0 para apoyar en el combate de la epidemia por COVID-19 a través de un dispensador para higiene de las manos usando dispositivos de construcción local

ARTICLE HISTORY

Received 30 September 2020
Accepted 16 October 2020

Andrés Ganán
Scitech Lab
Departamento de investigación y prototipos
Quito, Ecuador
andres.ganan@scitech-lab.com
https://orcid.org/0000-0001-9781-6214

Cristian Ganán
Scitech Lab
Departamento de investigación y prototipos
Quito, Ecuador
cristian.ganan@scitech-lab.com
https://orcid.org/0000-0002-5692-8495

Robert Enríquez
Universidad Central del Ecuador
Facultad de Ingeniería y Ciencias Aplicadas, Carrera de Sistemas de Información
Quito Ecuador
renriquez@uce.edu.ec

Use of Technology in Industry 4.0 to support the fight against the COVID-19 epidemic through a hand hygiene dispenser using locally built devices

Uso de la Tecnología en Industria 4.0 para apoyar en el combate de la epidemia por COVID-19 a través de un dispensador para higiene de las manos usando dispositivos de construcción local

Use of Technology in Industry 4.0 to support the fight against the COVID-19 epidemic through a hand hygiene dispenser using locally built devices

Andrés Ganán
Scitech Lab
Departamento de investigación y prototipos
Quito, Ecuador
andres.ganan@scitech-lab.com

Cristian Ganán
Scitech Lab
Departamento de investigación y prototipos
Quito, Ecuador
cristian.ganan@scitech-lab.com

Robert Enríquez
Universidad Central del Ecuador
Facultad de Ingeniería y Ciencias Aplicadas
Carrera de Sistemas de Información,
Quito Ecuador
renriquez@uce.edu.ec

Resumen — El surgimiento de la pandemia del COVID-19 generó una serie de problemas que debieron ser rápidamente resueltos sin contar con todos los recursos disponibles debido a las restricciones y las limitaciones impuestas. El trabajo presenta una innovación en el desarrollo de un prototipo que permite la desinfección de las manos por medio de líquidos que contienen alcohol sin la necesidad de que el usuario entre en contacto directo con el dispositivo, adaptado a la realidad ecuatoriana con partes que se pueden producir localmente. Se plantean los retos que se superaron para tener un prototipo funcional, incluyendo el diseño de los dispositivos de censado y actuación que se escogieron para cumplir con los objetivos planteados, así como la estructura de control, incluyendo las recomendaciones para su correcto uso y las propuestas para la mejora del dispositivo mediante la utilización de los elementos del internet de las cosas (IoT).

Palabras clave — *desinfección, dispensador automático, sensores y actuadores, manufactura aditiva*

Abstract — The outbreak of COVID-19 pandemic promoted the existence of new issues. They should have been quickly solved. The solutions have been promoted without all the available resources because lockdown and several restrictions that were established. This paper proposes an innovative idea with the development to get a functional prototype. The prototype allows the sanitation of hands. This process is gathered employing liquids that have alcohol. The dispenser does not require the direct contact of the user with the prototype. This is adapted to Ecuadorian reality and could be produced with local parts. We present the challenges that were solved to have a product that complete works. It includes the design of sensing and actuation devices that are chosen to achieve the projected goals. The control structure and the recommendations for correct usage are also presented. Finally, the proposals to have a better prototype with internet of things (IoT) are introduced.

Keywords — anitation, automatic dispenser, sensors and actuators, additive manufacturing

ISSN: 1390 -9266 – 2020 LAJC

A. Ganán, C. Ganán and R. Enríquez, "Uso de la Tecnología en Industria 4.0 para apoyar en el combate de la epidemia por COVID-19 a través de un dispensador para higiene de las manos usando dispositivos de construcción local", Latin-American Journal of Computing (LAJC), vol. 7, no. 2, 2020.

I. INTRODUCCIÓN

El lavado continuo y efectivo de las manos se ha mostrado como una forma muy simple y adecuada de controlar el esparcimiento de las infecciones, no solamente en ambientes controlados de tratamientos médicos, sino también en situaciones más cotidianas como en la preparación de alimentos, al ingresar en propiedades comerciales y/o de aglomeración. Para un correcto lavado y desinfección de las manos se requiere la utilización de líquidos que tienen las propiedades adecuadas para permitir la eliminación de los agentes infecciosos, acompañados de una correcta técnica de lavado de las manos [1][2].

Esta necesidad se hizo aún más relevante debido al aparecimiento súbito del virus SARS-CoV2 causante de la enfermedad coronavirus 2019 (COVID-19), surgido en China. El COVID-19 tuvo una rápida propagación global que ha causado que grupos enteros de poblaciones deban cumplir con largos periodos de aislamiento para tratar de reducir su propagación. Este virus tiene efectos potencialmente mortales en el sistema respiratorio y otras consecuencias que aún se encuentran en investigación, causantes de gran cantidad de pérdidas humanas desde que la enfermedad surgió, sin que exista aún un tratamiento completamente probado o una forma de prevenir la mencionada afección, teniendo datos que para mediados de agosto de 2020 la cantidad de personas contagiadas alcanzó más de 21 millones de casos confirmadas. Otra preocupación para los países es el evitar una sobredemanda de los servicios hospitalarios [3][4].

Se han establecido diversos mecanismos con el fin de contener los contagios masivos, a lo que se le añaden medidas de cumplimiento obligatorio que incluye la correcta desinfección de superficies, el respeto al distanciamiento social, el uso de mascarilla y protectores, así como el continuo lavado de manos o colocación de alcohol o soluciones en gel para las manos. La colocación de este tipo de líquidos se volvió especialmente necesaria para permitir el acceso de las personas a centros de abastecimiento de víveres, medicinas y productos de primera necesidad. Para minimizar los riesgos de contagio se plantea el establecimiento de una estrategia en la que el contacto con superficies sea limitado o se reduzca al máximo la utilización de elementos que constantemente son tocadas por las personas incluyendo botones de ascensores, escaleras mecánicas, en las que el riesgo de contagio puede elevarse [5].

El rápido surgimiento de la pandemia del COVID-19 planteó necesidades urgentes a cubrir, sabiendo que existieron varias barreras como son la escasez de los recursos disponibles, así como la falta de experiencias; permitió la adopción de una serie de tecnologías emergentes y disruptivas capaces de superar tales obstáculos, procurando siempre que el ingenio y la creatividad permitan la existencia de un entorno más seguro para continuar con las actividades cotidianas y productivas, sabiendo que las medidas de bioseguridad deberán ser atendidas durante tiempo indefinido hasta que la pandemia pueda ser controlada o exista una forma de generar inmunidad a la nueva enfermedad [6].

Aun sabiendo que las medidas de prevención del contagio en ambientes cerrados y espacios interiores, no mitigan por completo la posibilidad de contraer la enfermedad, es importante su implementación debido a que existe un número significativo de personas que no presentan ningún síntoma (asintomáticas) o que contrajeron la enfermedad en forma reciente. Tales medidas incluyen la higiene constante, la modificación de los espacios comerciales, así como las restricciones de ocupación de ambientes [7].

Los controles pueden incluir prácticas que son meramente administrativas y otras en las que la ingeniería y la tecnología son primordiales, dentro de las últimas se encuentra la implementación de estaciones y espacios que permiten el lavado e higiene de las manos y que también permiten la separación de elementos desinfectados de aquellos que han sido sometidos a procesos de limpieza, sabiendo que las manos tiene un rol representativo en la transmisión de enfermedades infecciosas, especialmente cuando se producen contactos cercanos con otras personas y objetos como pueden ser los mecanismos de apertura y cierre de puertas [7]. Según [8] uno de los métodos estandarizados para la eliminación de microorganismos consiste en la utilización de agentes desinfectantes basados en alcohol para las manos, esto debido a su eficiencia, aplicabilidad y tolerabilidad, teniendo pocos efectos adversos entre los que se incluye la resequedad de las manos. Otras soluciones incluyen la utilización de medios de desinfección en aerosol, soluciones químicas con amonio cuaternario, por nombrar otra que pueden resultar dañinos al contacto directo con la piel.

Los mecanismos que se han desarrollado para dispensar líquidos que permiten la desinfección de las manos y la piel de los seres humanos incluyen el uso de un elemento de accionamiento del dispensador con el pie, donde

el movimiento del pie permite la obtención de la fuerza mecánica y por medio de otros elementos tal movimiento es transmitido para que el líquido sea entregado al usuario. Una de las grandes barreras de esta propuesta podría suponer el impedimento de utilización por parte de personas que no tengan la fuerza suficiente, incluyendo adultos mayores e infantes [5].

Otro método que ha sido desarrollado involucra la utilización de microcontroladores con programación como son las tarjetas de desarrollo tipo Arduino, así como la utilización de un servomotor que se activa en función de las líneas de código establecidas para la activación de un dispensador tradicional, reemplazando la manipulación directa con las manos del dispensador con el uso de sensores y actuadores. Uno de los problemas de esta aproximación es el tiempo requerido para obtener la respuesta deseada por parte de los actuadores, así como la posibilidad de que el elemento de actuación sufra daño físico debido al constante estrés mecánico al que está siendo sometido, limitando la cantidad de veces que se puede emplear el prototipo sin necesidad de una recalibración y mantenimiento [5].

El trabajo documentado en [9] consiste en un conjunto de cuatro dispensadores que se colocan en conjunto con mecanismos de separación unos con otros formando una cruz donde en forma centralizada se presenta un depósito de líquido y un sistema de distribución que incluye válvulas solenoides, para un rellenado autónomo de cada dispensador, cámaras digitales, sensores ultrasónicos, así como una estructura de control basado en microcontroladores que permiten que cada dispensador sea controlado en forma independiente y cuya activación depende de servomotores y mecanismos de piñones y cremalleras. Toda esta estructura está destinada para uso institucional y requiere una elevada inversión para ser implementada, aunque plantea propuestas relevantes como son la inclusión de una cámara para la supervisión de la higiene o la utilización de mecanismos hidráulicos de rellenado del líquido a dispensar.

El prototipo propuesto en [10] emplea censado electrónico, una bomba de succión, microcontrolador y relés como elementos de activación, de tal forma que los elementos de actuación funcionen en forma rápida y precisa, conteniendo también señales de control de frecuencia elevada, en este caso los autores revisaron su funcionamiento durante el día completo sin tener problemas significativos en una semana, con un bajo consumo de energía, reduciendo el riesgo de contagio pero sabiendo que ciertos elementos incrementan el costo de implementación del prototipo en cuestión.

La propuesta de este trabajo toma en cuenta lo mencionado obteniendo una alternativa que dispensa el líquido sin contacto y que se implementó con recursos limitados en el contexto de la pandemia de COVID-19, empleando una metodología que condujo a la utilización de elementos producidos en forma local y que planteó como uno de sus objetivos una reducción de los costos asociados a los materiales a emplearse cumpliendo con la dispensación de líquidos. En esta primera fase; otro objetivo planteado es la reducción del tiempo necesario para la obtención de un producto final ya que no se tiene tiempos de espera entre la adquisición de materiales y la implementación, estos tiempos están ligados a la importación, transporte y otras componentes logísticas que suponen la utilización de elementos comerciales en mercados distantes, reduciendo así la dependencia tecnológica con otros mercados. El presente proyecto en su fase inicial está dirigido a dispensar líquidos con baja viscosidad debido al tipo de bomba de succión que fue diseñada y su capacidad limitada. El documento además plantea para trabajos futuros las posibilidades de mejora mediante la utilización de componentes de comunicación, formando otros dispositivos emergentes tipo IoT o que podrían contener inteligencia artificial (IA) para mejorar los hábitos de higiene. Esta es una segunda etapa del presente proyecto y que no se implementó debido a la imposibilidad de obtener los materiales necesarios para esta segunda fase.

Este documento tiene la siguiente organización: la sección II se revisa la metodología empleada, con énfasis en el desarrollo de los dispositivos con métodos de fabricación y prototipado rápido. La presentación del procedimiento de diseño de los elementos que debido a la escasez de recursos fueron construidos se aborda en la sección III, para cumplir con las necesidades del prototipo, así como la selección de dispositivos escogidos. La sección cuatro explica el funcionamiento de la solución propuesta, mientras que la quinta sección establece los resultados alcanzados, incluyendo las propuestas que se podrían establecer para mejorar el presente prototipo, convirtiéndolo en alternativas con inteligencia y que se convierten en soluciones de IoT. La sección VI presenta las conclusiones del presente trabajo.

ISSN: 1390 -9266 – 2020 LAJC

II. MÉTODO

En la actualidad se dispone de tres principios fundamentales para proceso de manufactura, el primero hace mención al proceso requerido para obtener un elemento de determinada geometría al extraer cantidades específicas de material por medio de fresado o rotación y toma el nombre de manufactura sustractiva, en segundo momento se hace mención a la manufactura de formación misma que hace uso de técnicas de forjado, doblado, entre otras al aplicar calor o fuerza y toma el nombre de manufactura formativa mientras que el último proceso recibe el nombre de manufactura aditiva mismo que basa sus procesos en la adición de material en formas específicas. En un primer instante los aspectos constructivos tienen relación con el mecanizado de piezas metálicas, pero también cuenta con procesos como el diseño por computador (CAD) y la utilización de métodos aditivos de manufactura para ciertos componentes del presente prototipo, así como la implementación de elementos de control transistorizado que se basan en señales digitales provenientes de elementos de censado [1][2].

A. Fabricación aditiva

Los procesos de manufactura por capas han estado presentes desde 1980 cuando estas tecnologías tomaron el nombre de prototipado rápido. Tales técnicas fueron implementadas para el desarrollo o construcción de prototipos iniciales que ahorraban una cantidad considerable de tiempo y dinero. Gracias a la madurez de la tecnología actualmente se usan plásticos, metales, cerámicas e incluso comida, hueso o tejido humano. Esta nueva tecnología también es usada en procesos de producción [1][2].

Es importante tomar en consideración que existen tres aplicaciones fundamentales de la técnica en cuestión, la primera denominada prototipado rápido (PR), utilizada para representar un producto en fase experimental para ser sometido a pruebas, la segunda aplicación consiste en fabricación rápida (FR) y es utilizada en la construcción de partes finales o productos listos para ser colocados en el mercado, la tercera aplicación consiste en la realización de herramientas, accesorios para herramientas e incluso dispositivos de medida [1][2].

B. Modelado por deposición fundida (Fused Deposition Modeling, FDM)

Es una de las técnicas con más estructuras implementadas en tareas de prototipado rápido. Su funcionamiento se basa en la creación de capas de plástico derretido una encima de otra. Dada la necesidad de la construcción por capas es necesario el procesamiento de los diseños en 3D por medio de un software encargado de dividir los sólidos en múltiples secciones horizontales que forman contornos bidimensionales. El proceso de fabricación contempla el paso del filamento por un elemento de calentamiento, luego el elemento plástico pasa por un extrusor y es depositado en una superficie plana. Las impresoras 3D actualmente basan su funcionamiento en el principio antes mencionado [1][2].

C. Selección de método

La metodología para el presente proyecto parte de la realización de iteraciones sucesivas de diversos mecanismos de actuación, por medio de la realización de ensayos y pruebas en sistemas que hacen uso de la manufactura aditiva, además del diseño conceptual y de detalle de los sistemas de control.

Por lo antes expuesto y entendiendo que la manufactura aditiva con la técnica FDM es ideal para tareas de prototipado rápido, se selecciona esta técnica para la elaboración iterativa de los componentes del actuador necesario para dispensar los líquidos sanitizantes. Por otro lado, las estructuras contenedoras del sistema se plantean para que sean diseñadas y construidas por medio de técnicas sustractivas y de formación con materiales resistentes, pero a la vez llamativos visualmente con la finalidad de obtener un producto de calidad ajustados por completo a la necesidad del actuador, contenedor y sistemas de control.

La estructura contenedora no se plantea como un proceso de iteraciones sucesivas dado que se propone un modelo estándar de dimensiones adecuadas con la finalidad de simplificar los procesos de producción, por ello desde el diseño hasta la concepción del sistema definitivo la estructura planteada no fue modificada.

Finalmente, la metodología planteada, para el diseño y ejecución del sistema de control, contempla la aplicación práctica de

teorías básicas de control con un sistema todo o nada de la mano de electrónica analógica. Al igual que lo mencionado para el contenedor del sistema, se elimina la necesidad de iteraciones sucesivas. Esto se debe a que el planteamiento inicial radica en el uso de sistemas plenamente probados y desarrollados con anterioridad, por lo cual, el diseño inicial se mantendrá sin alteraciones para la duración del desarrollo y construcción final.

III. PROCEDIMIENTO

El presente proyecto fue ejecutado durante el período de aislamiento obligatorio, motivo por el cual los recursos disponibles resultaron limitados. En este sentido la fabricación digital aditiva, específicamente FDM que se trató en la sección previa, así como la metodología planteada, resultaron fundamentales para la obtención del prototipo dispensador.

Parte de los esfuerzos realizados tienen directa relación a la obtención de un actuador capaz de impulsar líquidos en el momento correcto en función de lo que solicita la estructura de control establecida y los sensores colocados. Esta construcción permite la obtención de una micro bomba de succión basada en un motor de DC y una estructura de absorción con diseño computarizado (CAD) e impresa en 3D mediante técnica de modelado por FDM [9] [11].

El prototipo de actuador está realizado de tal forma de no ser de tipo inmersivo, con el fin de no correr riesgos de disrupciones eléctricas en materiales inflamables como son los líquidos de desinfección.

Los prototipos de actuación además debieron ser sometidos a procesos que los hermetizan para reducir la posibilidad de fuga de los líquidos hacia los componentes electrónicos. También se debe recalcar que el prototipo fue diseñado para ser acoplado a diversos envases y recipientes contenedores del líquido a ser aplicado.

La figura 1 muestra los modelos en 3D correspondientes a la parte rotativa de la bomba miniatura centrífuga, así como su carcasa y estructuras de conexión hacia elementos de circulación del líquido. Estas piezas son el resultado de la metodología de iteraciones sucesivas y son fabricadas por medio de la técnica FDM.

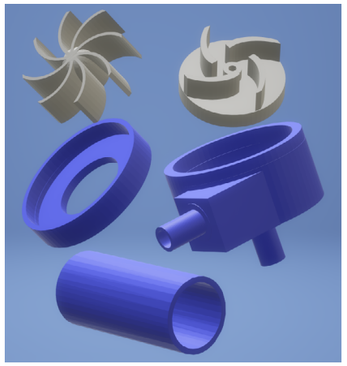


Fig. 1: Estructuras diseñadas del prototipo de mini bomba de succión

A. Selección de dispositivos

El rendimiento de un sistema que se encuentra en fase de desarrollo es un factor a considerar. La influencia se da en la elección del sensor que se adapta a las condiciones de operación del sistema. Sin duda la selección de un sensor conlleva también el análisis de la relación rendimiento-precio, así por ejemplo el dispositivo que es objeto de la presente investigación podría considerar incluso sistemas de visión artificial o robustos sistemas de medición y detección láser que mejoren el funcionamiento del prototipo [12].

1. Sensor Infrarrojo (IR)

El sensor infrarrojo para detección de obstáculos basa su funcionamiento en dos componentes de silicio, en primer lugar, se dispone de un diodo LED que emite luz infrarroja y un segundo componente encargado de receptar la reflexión de la luz infrarroja. El segundo elemento, siendo el más importante, produce un voltaje en sus terminales por efectos fotoeléctricos. La detección del obstáculo entonces depende de la existencia de un objeto que permita reflejar la luz infrarroja.

El sensor infrarrojo propuesto posee un circuito comparador compuesto por un amplificador operacional interno que en función de la calibración seleccionada genera una salida

ISSN: 1390 -9266 – 2020 LAJC

digital. El potenciómetro permite una regulación de distancia de detección teórica de entre 2 y 30 centímetros con un ángulo de detección de 35°. El sensor en mención puede ser conectado directamente a un microcontrolador o manejar el control de un relé o elemento de potencia. Otra gran ventaja radica en el tamaño del dispositivo dado que tan sólo mide 3.2 centímetros por 1.4 centímetros, el funcionamiento del sensor infrarrojo reflectivo se muestra en la Fig. 2.

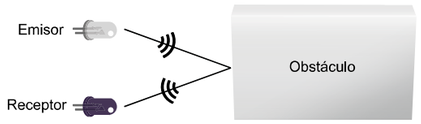


Fig. 2: Principio de operación sensor infrarrojo

2. Dispositivo de potencia

El elemento de potencia propuesto corresponde a un transistor de tipo NPN. Está configurado para que opere de manera análoga a un interruptor. Dado que opera en la zona de avalancha, el elemento en mención deberá ser capaz de manejar la corriente y voltaje requeridos por la bomba de succión a ser implementada, mientras que, los valores de activación en la base deberán ser consistentes con aquellos brindados por el sensor infrarrojo. Debido a que los valores de funcionamiento del sensor podrían significar un inconveniente, se propone el uso de un transistor especial denominado Darlington, con el cual es posible manejar corrientes relativamente elevadas con una corriente pequeña. El uso de este transistor es importante para trabajar con motores en condiciones de operación especiales [13].

B. Solución Propuesta

En función de lo antes expresado, se propone un dispositivo capaz de detectar la presencia y cercanía de las manos del usuario frente al ducto del dispensador. Al detectar las manos, de manera automática provoca un flujo continuo de líquido sanitizante desde el contenedor principal hasta la salida del sistema hidráulico. La cantidad de líquido a requerir es decisión del usuario dado, que al retirar las manos el sistema se apagará y el flujo de líquido se detendrá. La fig. 3 muestra el esquema del sistema propuesto.

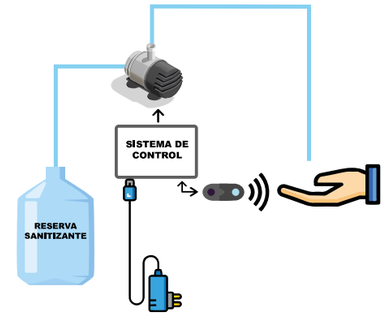


Fig. 3: Esquema funcional

1. Circuito de control

El elemento de potencia propuesto corresponde a un transistor de tipo NPN. Está configurado para que opere de manera análoga a un interruptor. Dado que opera en la zona de avalancha, el elemento en mención deberá ser capaz de manejar la corriente y voltaje requeridos por la bomba de succión a ser implementada, mientras que, los valores de activación en la base deberán ser consistentes con aquellos brindados por el sensor infrarrojo. Debido a que los valores de funcionamiento del sensor podrían significar un inconveniente, se propone el uso de un transistor especial denominado Darlington, con el cual es posible manejar corrientes relativamente elevadas con una corriente pequeña. El uso de este transistor es importante para trabajar con motores en condiciones de operación especiales [13].

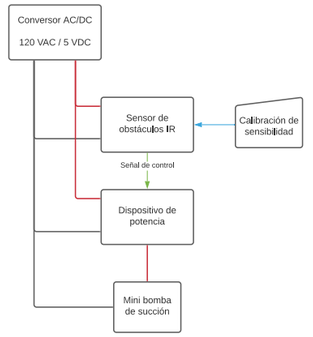


Fig. 4: Esquema sistema de control.

2. Características de los elementos

El sensor infrarrojo utilizado cuenta con las características listadas en la tabla I. El sensor mencionado es ensamblado por múltiples fabricantes, pero las características de

operación son similares. El sensor se alimenta de un voltaje que se puede obtener de dispositivos USB o de baterías de litio que actualmente son ampliamente difundidas.

TABLA I. PARÁMETROS SENSOR INFRARROJO

Parámetro	Valor	Unidad
Voltaje de operación	3.3 - 5	V
Rango	2 - 30	cm
Ángulo de detección	35	°
Circuito comparador	LM393	N.A.
Calibración	Potenciómetro	N.A.
Indicadores	Detección / Alimentación	N.A.
Compatibilidad	Arduino, AVR, PIC, microcontrolador	N.A.

El dispositivo seleccionado, para manejar las funciones de potencia y para controlar el motor, es un transistor TIP127 de tipo Darlington y configuración PNP. Los datos más importantes del dispositivo son mostrados en la tabla II. En esta se mencionan únicamente las características operativas.

TABLA II. PARÁMETROS ELEMENTO DE POTENCIA.

Parámetro	Valor	Unidad
Voltaje Colector-Base	-100	V
Voltaje Colector-Emisor	-100	V
Voltaje Emisor-Base	-5	V
Corriente de colector	-5 -8	A
Corriente de base	-120	mA

Con el fin de acoplar el sensor con el dispositivo de potencia se utiliza una resistencia de 1000 ohmios entre el terminal de salida del sensor y la base del transistor. Como pudo verse en la tabla II, la corriente de base del dispositivo seleccionado es baja.

Como se mencionó en párrafos anteriores la bomba fue ensamblada usando una impresora 3D y se seleccionó como material el PLA. Debido al proceso y tareas que van a realizar las piezas se optó por utilizar un 100% de relleno en las piezas mientras que el espesor de capa seleccionado fue 0.2 milímetros.

Por otro lado, el motor seleccionado para el ensamblaje de la bomba es un micromotor sin núcleo. Este tipo de motor es comúnmente utilizado en drones debido a su reducido tamaño, robustez, facilidad de conexión y alta velocidad. Estos motores operan a 63000 revoluciones por minuto. La tabla III muestra las principales características del motor en mención.

TABLA III. PARÁMETROS MICROMOTOR.

Parámetro	Valor	Unidad
Tipo de corriente	DC	N.A.
Voltaje de diseño	3.7	V
Velocidad sin carga	63855	rpm
Voltaje nominal	3.7	V
Corriente sin carga	20	mA
Tipo de eje	Directo	N.A.
Diametro del eje	0.8	mm
Longitud del eje	3.5	mm
Dimensión	6x12	mm

IV. RESULTADOS Y DISCUSIÓN

La presente sección muestra al dispositivo obtenido en la primera fase del proyecto. El dispositivo contiene todos los elementos antes descritos. En la Fig. 5 se muestran las dimensiones proyectadas del prototipo se observa la forma del contenedor o de la cubierta exterior, la botella o el recipiente provisto para el líquido de desinfección y la cavidad provista para la salida del componente sanitizante. Cada estructura cuenta con sus respectivas medidas.

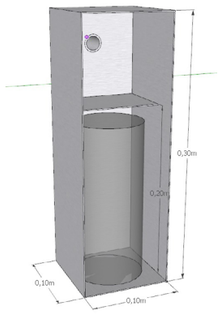


Fig. 5: Modelo de la estructura exterior del prototipo de dispensador sin contacto

ISSN: 1390 -9266 – 2020 LAJC

La fig. 6 muestra el prototipo en su versión final, con un acabado metálico. Se puede observar que apenas se nota la salida del elemento de censado infrarrojo y la apertura que permite la salida del líquido. El dispositivo es ideal para colocarse en cualquier superficie; su estructura está establecida para poder ser modificada. Se pueden colocar al dispositivo elementos que mejoren la funcionalidad tal y como se presentará en lo sucesivo.

Fig. 6: Vista del prototipo de dispensador sin contacto construido

El dispositivo cumple con la función de dispensar el líquido desinfectante en función del tiempo que coloca el usuario sus manos en frente del sensor provisto para el efecto. El dispensador presentado es el resultado de la revisión del estado del arte disponible. Como resultado del método planteado, la fig. 7 ilustra la división por partes de la bomba ensamblada, cuyas piezas son el resultado de un proceso de fabricación por FDM, en conjunto con el motor DC seleccionado como elemento motriz. Respecto a la fig. 1 se puede notar que fue seleccionada la hélice de la de la zona superior izquierda, descartando la segunda opción al no cumplir la función requerida. La dimensión reducida del motor trae consigo que las dimensiones finales de la bomba también sean mínimas en comparación a otras opciones comerciales.

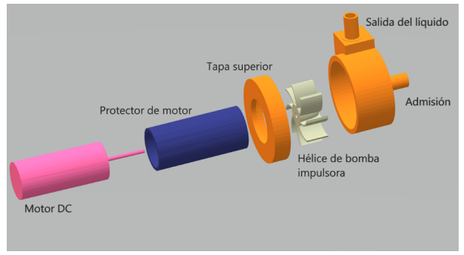


Fig. 7: División en partes, bomba impulsora de líquido.

Por otro lado, el circuito impreso correspondiente al control del dispensador se puede observar en la fig.8. Se destaca que la figura muestra el diseño final en 3D con una dimensión reducida, con el fin de que la placa sea sencilla de colocar en el prototipo. Los elementos ilustrados en color celeste representan borneras, estos componentes se colocan para facilitar el mantenimiento o reparación del dispositivo en caso fortuito.

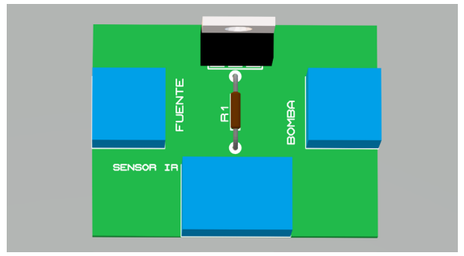


Fig. 8: División en partes, bomba impulsora de líquido.

V. TRABAJOS FUTUROS

En la presente sección se establecen ciertos aspectos que se tomarán en cuenta para la mejora del dispositivo en una segunda fase, tomando en cuenta los requerimientos de los dispositivos tecnológicos emergentes frente al auge de la industria 4.0 y del IoT. La inclusión de esta clase de tecnología; mejora el control, la comunicación y la seguridad con la que se manejan los dispositivos. Tales mejoras permiten un nivel en que las tecnologías digitales y la automatización trabajan en conjunto. Ello promueve la combinación de diversas tecnologías y la creación de un sinnúmero de oportunidades de valor [14].

La propuesta se podría ampliar a otros tipos de líquidos y geles de desinfección colocando otra clase de bombas como son las de tipo peristáltico. Lo que se busca es ampliar la aplicación del dispositivo. Otras aplicaciones podrían implicar la utilización de mecanismos más robustos de censado y actuación, así

como un sistema de procesamiento para obtener datos y estadísticas relacionadas a la utilización del dispositivo. Para complementar el funcionamiento, una de las propuestas consiste en la colocación de una estructura capaz de monitorear y entregar información al usuario respecto al uso del dispositivo. Entre la información que se puede obtener se encuentra la necesidad de reposición del líquido, la cantidad de veces que el dispositivo fue activado, y el tiempo promedio en que un usuario tomó líquido en sus manos. Estas métricas podrían ayudar a un mejor uso del dispositivo por medio de recomendaciones a los usuarios respecto al tiempo ideal de uso que permita una correcta higiene de las manos, pero a la vez evite el desperdicio de los recursos. Los sistemas de alerta para los encargados de mantenimiento de las estaciones de desinfección del agotamiento del líquido sanitizante también podrían ser implementados para mantener la disponibilidad del sistema dispensador la mayor parte del tiempo.

La otra propuesta que se plantea es el uso de visión artificial e inteligencia artificial. Estos sistemas servirían para indicar al usuario si se realizó una correcta higiene de las manos, o en caso contrario presentarle alternativas de mejora o un esquema educativo respecto a las recomendaciones de los entes competentes de la salud respecto a la forma correcta de realizar el lavado de las manos. El sistema requiere una estructura de procesamiento más robusta centralizada en el dispositivo; su aplicación podría estar dispuesta para lugares en los que la correcta higiene de las manos es fundamental como por ejemplo los centros de atención de la salud, así lugares de manipulación de los alimentos, etc. Por otro lado, el sistema podría contar con la posibilidad de un sistema para autenticación y reconocimiento del usuario. El reconocimiento permite la promoción de un programa continuo de mejora de las prácticas en la higiene de las manos. Tal procedimiento será fundamental para el ingreso a ambientes cerrados.

VI. CONCLUSIONES

El presente documento establece la relevancia que tiene la realización de dispositivos y prototipos que pueden ser implementados con facilidad. En el contexto específico de la pandemia del coronavirus fueron el resultado de la utilización de diversas tecnologías. Entre los procesos están la manufactura aditiva y técnicas de mecanización. Para cumplir con las funciones se usan elementos de fácil adquisición y que, en forma efectiva dispensan desinfectantes a los usuarios en zonas de acceso a ambientes interiores.

La estructura planteada usa sensores y actuadores tradicionales combinados con técnicas de producción específicas. Esta unión da lugar a necesidades como el diseño de equipos de actuación que evitan problemas asociados a la disrupción eléctrica o la existencia de fugas de los líquidos, El trabajo armónico da lugar a una aplicación específica de los componentes elegidos y diseñados.

Los eventos súbitos, como la aparición de una nueva enfermedad, plantean desafíos que requieren una respuesta rápida de parte de los investigadores y espacios de creación para plantear alternativas de fácil implementación con los recursos disponibles. El planteamiento de oportunidades de mejora empleando tecnologías emergentes para convertirlos en dispositivos inteligentes y ajustados a las necesidades de brindar información y estadísticas de su uso de tal forma de poder ajustarlos a la realidad y el contexto de utilización de determinada industria. También se puede complementar su utilidad con funciones adicionales como la mejora de los hábitos y prácticas de determinado grupo poblacional, contribuyendo más allá de la utilidad práctica inicialmente establecida.

Una vez las restricciones fueron superadas, la conversión del dispositivo por medio de tecnología IoT está siendo ejecutada. El dispensador en la presente propuesta puede ser mejorado empleando datos y métricas que se obtengan de su uso. La constante utilización permitirá además la distinción de desafíos en tópicos como la seguridad de los datos sabiendo que ciertas métricas tienen directa relación a la identidad de los individuos.

ISSN: 1390 -9266 – 2020 LAJC

VII. REFERENCIAS

[1] D. F. Llorca, I. Parra, M. Á. Sotelo, and G. Lacey, “A vision-based system for automatic hand washing quality assessment,” Mach. Vis. Appl., vol. 22, no. 2, pp. 219–234, 2011.
[2] S. Bánsághi, H. Soule, C. Guitart, D. Pittet, and T. Haidegger, “Critical Reliability Issues of Common Type Alcohol-Based Handrub Dispensers,” Antimicrob. Resist. Infect. Control, vol. 9, no. 1, pp. 1–13, 2020.
[3] M. Tropea and F. De Rango, “COVID-19 in Italy: current state, impact and ICT-based solutions,” IET Smart Cities, vol. 2, no. 2, pp. 74–81, 2020.
[4] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, “A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact,” IEEE Access, vol. 8, no. April, pp. 90225–90265, 2020.
[5] M. M. Srihari, “Self-Activating Sanitizer With Battery Imposed System For Cleansing Hands,” 2020 Second Int. Conf. Inven. Res. Comput. Appl., pp. 1102–1105, 2020.
[6] S. Agarwal et al., “Unleashing the power of disruptive and emerging technologies amid COVID-19: A detailed review,” 2020.
[7] T. Chen and J. O. Keeffe, “COVID-19 in indoor environments — Air and surface disinfection measures Prepared by Current approaches to risk mitigation in indoor spaces,” pp. 1–25, 2020.
[8] A. Banik, “Portable Integrated Hand Sterilizer and Dispenser to Ensure Hand Hygiene and Subsidized Facial Mask,” SSRN Electron. J., 2020.
[9] A. Gebhardt and J.-S. Hötter, Additive Manufacturing: 3D Printing for Prototyping and Manufacturing, vol. 35, no. 3. 2016.
[10] A. Gupta, “Novel design of automatic sanitizer dispenser machine based on ultrasonic sensor,” no. September, 2020.
[11] K. Upadhyay, R. Dwivedi, and A. K. Singh, “Determination and Comparison of the Anisotropic Strengths of Fused Deposition Modeling P400 ABS,” in Advances in 3D Printing & Additive Manufacturing Technologies, vol. 21, no. 46, Singapore: Springer Singapore, pp. 9–28, 2017.
[12] B. Mustapha, A. Zayegh, and R. K. Begg, “Ultrasonic and infrared sensors performance in a wireless obstacle detection system,” Proc. - 1st Int. Conf. Artif. Intell. Model. Simulation, AIMS 2013, pp. 487–492, 2014.
[13] S. W. Amos and M. James, “Principles of transistor circuits: introduction to the design of amplifiers, receivers, and digital circuits”, Newnes, 2000.
[14] P. W. Chan, “Briefing: Industry 4.0 in Construction: Radical Transformation or Restricted Agendas?,” Proc. Inst. Civ. Eng. - Manag. Procure. Law, pp. 1–4, 2020.

AUTHORS

Andrés Ganán

Nació en Quito-Ecuador el 28 de Julio de 1995. Realizó sus estudios en la Universidad Politécnica Salesiana en donde obtuvo su título en Ingeniería Eléctrica. Tiene experiencia en modelamiento matemático de redes eléctricas, redes eléctricas inteligentes y programación multilenguaje enfocado al desarrollo de productos y prototipos por medio de fabricación aditiva y dispositivos electrónicos inteligentes. Actualmente se desempeña como investigador en Scitech.

Cristian Ganán

Nació en Quito-Ecuador el 6 de Julio de 1992. Realizó sus estudios en la Universidad Politécnica Salesiana en donde obtuvo su título en Ingeniería Eléctrica y además formó parte del grupo de investigación en Redes Eléctricas (GIREI). Tiene experiencia en modelamiento matemático de redes eléctricas, redes eléctricas inteligentes y sistemas georreferenciados. Actualmente se enfoca en al desarrollo de productos y prototipos por medio de fabricación aditiva y dispositivos electrónicos inteligentes y se desempeña como investigador en Scitech.

ISSN: 1390 -9266 – 2020 LAJC

Robert Enríquez

Ingeniero Electrónico en Telecomunicaciones de la Escuela Politécnica Nacional, Maestría en Docencia Universitaria en la Universidad Central del Ecuador (´12), Especialista en Oil and Gas Industry Management en Saint Vincent College, USA (´13), Maestría en Gestión de las Comunicaciones y Sistemas de Información en la Escuela Politénica Nacional (´15), Doctor en Informática en la Universitat d´Alacant, España (´19). Ha sido docente por más de 22 años en varias universidades de Ecuador. Ha escrito más de 25 artículos referentes a gestión de tecnología, seguridades, datos abiertos. Ha dirigido 12 tesis de maestría y ha sido director del proyecto de datos abiertos de la Universidad Central del Ecuador. Actualmente es miembro de los proyectos UETIC y Ciberseguridad auspiciados por CEDIA. General Workshop Chair: Industry 4.0 y Cyberseguridad TIC EC CEDIA. Experiencia en la empresa pública como privada nacional e internacional, Gerente de Tecnología en varias empresas de la Industria de Finanzas y Petróleo.

A. Ganán, C. Ganán and R. Enríquez, "Uso de la Tecnología en Industria 4.0 para apoyar en el combate de la epidemia por COVID-19 a través de un dispensador para higiene de las manos usando dispositivos de construcción local", Latin-American Journal of Computing (LAJC), vol. 7, no. 2, 2020.

LATIN-AMERICAN JOURNAL OF COMPUTING

Published by

Escuela Politécnica Nacional
Facultad de Ingeniería de Sistemas
Quito-Ecuador

https://lajc.epn.edu.ec/
lajc@epn.edu.ec

December 2020

ISSN: 1390 -9266 – 2020 LAJC

Vol VII, Issue 2, December 2020

https://www.epn.edu.ec

QUITO - ECUADOR

LATIN-AMERICAN JOURNAL OF COMPUTING

Vol VII, Issue 2, December 2020