Nodos sensores y protocolos de comunicación del internet de las cosas aplicados a la agricultura inteligente

Chuchico Arcos, Cristian Paul

Departamento de Eléctrica y Electrónica

Maestría en Electrónica y Automatización Mención Redes Industriales

Trabajo de Titulación, previo a la obtención del título Magister en Electrónica y Automatización Mención Redes Industriales

Ing. Rivas Lalaleo, David Raimundo Ph.D.

Latacunga, 22 de noviembre de 2021

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Nodos sensores y protocolos de comunicación del internet de las cosas aplicados a la agricultura inteligente**" fue realizado por el señor **Chuchico Arcos, Cristian Paúl** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga, 22 de noviembre de 2021

DAVID RAIMUNDO RIVAS LALALEO

Firmado digitalmente por DAVID RAIMUNDO RIVAS LALALEO

Ing. Rivas Lalaleo, David Raimundo Ph.D.

Director

C.C.: 1802445302

RESULTADO DE ANÁLISIS URKUND

Curiginal

Document Information

Analyzed document	Tesis_Chuchico_Arcos_Cristian_Paul.pdf (D119599271)
Submitted	11/23/2021 12:53:00 PM
Submitted by	Juan Carlos Altamirano
Submitter email	jc.altamiranoc@uta.edu.ec
Similarity	7%
Analysis address	jc.altamiranoc.uta@analysis.urkund.com

Sources included in the report

W	URL: https://dialnet.unirioja.es/descarga/articulo/6720876.pdf Fetched: 11/23/2021 12:55:00 PM	6
SA	**DE_SALAZAR_MARTINEZ_QJ07336_20190904_1403_c033.pdf** Document DE_SALAZAR_MARTINEZ_QJ07336_20190904_1403_c033.pdf (D55268270)	7
W	URL: http://www.iiisci.org/journal/PDV/risci/pdfs/CA544SI17.pdf Fetched: 11/23/2021 12:55:00 PM	4
W	URL: https://enviraiot.es/sectores/smart-agro/ Fetched: 11/23/2021 12:55:00 PM	1
W	URL: https://lainholding.com/agricultura-de-precision-iot-sensores-inteligentes/ Fetched: 11/23/2021 12:55:00 PM	12
W	URL: https://la.mathworks.com/solutions/internet-of-things.html Fetched: 11/23/2021 12:55:00 PM	1
W	URL: https://repositorio.usm.cl/bitstream/handle/11673/49644/m18457744-5.pdf?sequence=1&isAllowed=y Fetched: 11/23/2021 12:55:00 PM	1

DAVID RAIMUNDO RIVAS LALALEO

Firmado digitalmente por DAVID RAIMUNDO RIVAS LALALEO

Ing. Rivas Lalaleo, David Raimundo Ph.D.

Director

C.C.: 1802445302

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Yo **Chuchico Arcos, Cristian Paúl**, con cédula de ciudadanía n° 0503062713, declaro que el contenido, ideas y criterios del trabajo de titulación*: "***Nodos sensores y protocolos de comunicación del internet de las cosas aplicados a la agricultura inteligente"** es de mí autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 22 de noviembre de 2021

Firmado digitalmente por:
CRISTIAN PAUL CHUCHICO ARCOS
Razón:
Localización:
Fecha: 2021-11-30T20:33:35.494-05:00

.....

Chuchico Arcos, Cristian Paúl

C.C.: 0503062713

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Chuchico Arcos, Cristian Paul** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: "**Nodos sensores y protocolos de comunicación del internet de las cosas aplicados a la agricultura inteligente"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 22 de noviembre de 2021

Firmado digitalmente por:
CRISTIAN PAUL CHUCHICO ARCOS
Razón:
Localización:
Fecha: 2021-11-30T20:33:35.494-05:00

.....

Chuchico Arcos, Cristian Paul

C.C.: 0503062713

DEDICATORIA

Este trabajo lo dedico con el más profundo sentimiento a mis padres Iván y Gladys, a mi novia y futura esposa Maydelinne y a mi hija Briana Arlette. Su amor incondicional, el regalo más grande que Dios me dio, ha sido mi inspiración para luchar por ser cada día mejor.

AGRADECIMIENTO

Agradezco a Dios por ser la luz y la fuerza para sobrellevar las dificultades del camino, agradezco a mi familia de manera especial a mis padres Iván y Gladys, a mi novia Maydelinne, quienes han estado y estarán presentes en cada peldaño de la vida.

A mis amigos Jonathan Vélez, Germánico Sinchiguano, Javier Heredia, Fernando Chicaiza, Adrián Ávila y Luis Tapia por brindarme siempre palabras de aliento, solidaridad y confianza; por compartir grandes momentos y ser ustedes quienes le dan el verdadero significado a la palabra amistad.

A mis profesores del programa de maestría por las enseñanzas impartidas, de manera especial al Ing. David Rivas quien fue artífice importante en el desarrollo del presente proyecto.

A todos ustedes mi eterna gratitud.

Tabla de Contenidos

Carátula **1**
Certificación 2
Resultado de análisis urkund 3
Responsabilidad de autoría 4
Autorización de publicación 5
Dedicatoria 6
Agradecimiento 7
Índice de Contenidos **8**
Índice de figuras…. **11**
Índice de Tablas…. **13**
Tabla de acrónimos **14**
Resumen **15**
Abstract **16**
Planteamiento del problema de investigación 17
Introducción 17
Justificación **20**
Hipótesis de investigación **21**
Antecedentes **21**
Objetivos **24**
Objetivo general del proyecto **24**
Objetivos específicos del proyecto **24**
Marco teórico 25
Introducción **25**
Internet de las cosas **26**
Tecnologías de Comunicación Para IoT **28**
Machine to machine GSM/GPRS **28**
SigFOX **29**
LoRa **29**
NarrowBand IoT **30**
Bluetooth Low Energy **30**
Zigbee **31**
Protocolos de Comunicación Para IoT **32**
Message Queue Telemetry Transport **32**

Constrained Application Protocol 33
Advanced Message Queuing Protocol 33
Simple/Streaming Text Oriented Messaging Protocol 34
Arquitectura IoT 34
Nodos Sensores 35
Red de Sensores 36
IoT y Fog computing 36
Seguridad en redes IoT 37
Ventajas y Desventajas del IoT 41
Agricultura Inteligente 42
IoT en la Agricultura 43
Beneficios de IoT en la Agricultura 44
Componentes Comerciales Aplicados en la Agricultura Inteligente 45
IoT Gateway Ethernet / MQTT – Converter HD67930-B2 45
Envira…… 46
Nanoenvi AG 46
Monitorización Meteorológica en Agricultura de Precisión 47
Monnit…… 48
Sensor inalámbrico de humedad (RH) ALTA 48
Sensor de velocidad de aire inalámbrico 49
Sensor inalámbrico de humedad del suelo 49
Libelium…… 50
Plug & Sense 50
Smart Environment PRO 51
Smart Agriculture Xtreme 52
Lain Holding 53
Estación Meteorológica 54
Sensor de humedad de hojas 54
Indicador de lluvia y precipitación 54
Sonda de humedad del suelo de capacitancia 54
Agricultura IOT inteligente XT: Sensores integrados 54
Análisis de herramientas de simulación para IoT 56
Análisis Bibliométrico 58
VOSviewer 58

Metodología de la Investigación 59
Experimentación y Resultados 61
Análisis bibliométrico **61**
Análisis del consumo energético **65**
Seguridad en los protocolos y arquitecturas de comunicación **69**
Descripción de Seguridad de Zig Bee **72**
Descripción de Seguridad de Bluetooth **73**
Descripción de Seguridad de LoRa WAN **74**
Descripción de Seguridad de NB IoT **74**
Carcasas y encapsulados de los nodos sensores **76**
Simulación como herramienta de análisis previo a la implementación **80**
Simulación CoAP **83**
Simulación MQTT **87**
Monitoreo de Parámetros de la Red **90**
Ejemplo de implementación de un servidor MQTT **98**
Validación de la hipótesis **105**
Conclusiones: 107
Recomendaciones 109
Bibliografía 110
Anexos 116

Índice de figuras

Figura 1. *Representación generalizada de una arquitectura de IoT.* 35
Figura 2. *Principales componentes de una estación de monitoreo.* 43
Figura 3. *Representación de la aplicación del Gateway Ethernet/MQTT.* 46
Figura 4. *Representación de una arquitectura Envira* 48
Figura 5. *Representación de una arquitectura Monnit* 50
Figura 6. *Representación de componentes Libelium.* 53
Figura 7. *Representación de componentes de la arquitectura Lain* 55
Figura 8. *Procedimiento de síntesis de información.* 59
Figura 9. *Número de publicaciones por años SCOPUS (IoT + Smart Agriculture).* 61
Figura 10. *Concentración de publicaciones por territorio* 62
Figura 11. *Visualización de red de términos asociados a IoT y agricultura inteligente.* 63
Figura *12*. *Visualización de superposición de términos asociados a IoT y agricultura inteligente* 63
Figura 13. *Visualización de densidad de clústers asociados a IoT y agricultura inteligente* 64
Figura 14. *Principales características de la seguridad de redes.* 76
Figura 15. *Ejemplo de carcasa impresa en 3D.* 77
Figura 16. *Contenedor plástico para nodo sensor.* 77
Figura 17. *Carcasa de protección para nodo sensor ubicado al ras del suelo.* 78
Figura 18. *Encapsulado comercial adaptable.* 78
Figura 19. *Script de intercambio de mensajes de saludo* 81
Figura 20. *Nodos sensores disponibles para simulación* 82
Figura 21. *Nodos sensores y propiedades para análisis durante la simulación.* 82
Figura 22. *Ejecución de la simulación, mensajes intercambiados.* 83
Figura 23. *Topología física de los nodos sensores para simulación* 84
Figura 24. *Ejecución del servidor y direcciones Ipv6.* 85
Figura 25. *Tráfico de datos generado por los nodos sensores.* 86
Figura 26. *Verificación de rutas y adyacencias en el servidor.* 86
Figura 27. *Escenario de simulación para protocolo MQTT.* 87
Figura 28. *Ingreso al directorio e instalación del servidor MQTT.* 88
Figura 29. *Tráfico de datos generados durante la simulación.* 89
Figura 30. *Mensajes en la inicialización de la simulación.* 89
Figura 31. *Topología física para el escenario de simulación de recopilación de datos.* 90
Figura 32. *Radio de cobertura del nodo servidor.* 91
Figura 33. *Topología lógica de la red.* 92
Figura 34. *Gráfica de consumo promedio de energía por nodo.* 93
Figura 35. *Número de saltos por cada nodo.* 94
Figura 36. *Métrica promedio del nodo 6.* 95
Figura 37. *Métrica promedio del nodo 10.* 95
Figura 38. *Métrica del nodo 12, donde se observa un recálculo de la misma.* 96
Figura 39. *Promedio de la métrica de todos los nodos sensores.* 96
Figura 40. *Número de vecinos por cada nodo.* 97
Figura 41. *Análisis de las métricas de cada nodo sensor.* 97
Figura 42. *Ejecución de Node-Red* 99
Figura 43. *Ejecución del servidor MQTT, Mosquitto.* 99

Figura 44. *Ingreso a la interfaz de configuración Node-Red.*.....100
Figura 45. *Ingreso a la interfaz del servidor desde una PC.* 101
Figura 46. *Ingreso a la interfaz del servidor desde un dispositivo móvil.* 101
Figura 47. *Programación desarrollada para la suscripción y publicación*. 102
Figura 48. *Valores recibidos en el servidor MQTT, tópico Var_Digital.* 103
Figura 49. *Valores recibidos en el servidor MQTT, tópico Set_Point*. 103
Figura 50. *Valores recibidos en el servidor MQTT, tópico Var_Analog.*.....104

Índice de Tablas

Tabla 1. *Ejemplos de aplicación de la recopilación y análisis de datos.* 25
Tabla 2. *Buenas prácticas de seguridad de red.* 39
Tabla 3. *Ejemplos de nodos sensores y consumo energético.* 66
Tabla 4. *Consumo energético de tarjetas controladoras utilizadas en IoT.* 67
Tabla 5. *Estimación de tiempo de vida de la batería de proyectos desarrollados.* 67
Tabla 6. *Descripción de términos asociados a la seguridad de redes.* 69
Tabla 7. *Ejemplos de ataques y acciones de mitigación.* 70
Tabla 8. *Características de seguridad de protocolos utilizados.* 75
Tabla 9. *Descripción de encapsulados y carcasas de protección de nodos sensores.* 79

Tabla de acrónimos

IoT:	Internet of things, internet de las cosas.
WSN:	Wireless network sensor.
6LoWPAN:	IPv6 over Low-Power Wireless ërsonal Area Networks.
M2M:	Machine to machine.
AMQP:	Advanced Message Queuing Protocol.
MQTT:	Message queue telemetry transport.
CoAP:	Constrained Application Protocol.
TLS:	Transport layer security.
SSL:	Secure socket layers.
SASL:	Simple Authentication and Security Layer.
STOMP:	Simple/Streaming text oriented messaging protocol.
PII:	Personally identifiable information.
SPI:	Sensitive personal information.
TCP:	Transmission control protocol.
UDP:	User datagram protocol.
AQI:	Air quality index.
LPM:	Low power mode.

Resumen

El desarrollo de la agricultura inteligente ha presentado en los últimos años un amplio desarrollo, razón por la cual alrededor del mundo se han presentado un sinnúmero de propuestas. Esta alta variabilidad de tecnologías usadas en la implementación en este tipo de soluciones ha generado en los usuarios cierta confusión de que tipos de equipos o protocolos de comunicación utilizar dependiendo el caso de aplicación. En este artículo se analizan los distintos trabajos y tecnologías usadas en IoT aplicado a la agricultura comparando sus características técnicas a través de análisis documental, simulaciones de casos de estudios, entre otros. Tras este estudio se describe por medio de tablas los resultados obtenidos de la revisión bibliográfica y documental, además se reproduce nodos sensores con las características técnicas específicas como son su protocolo de comunicación, el consumo de energía, grados de protección de los dispositivos, seguridad de las redes implementadas, entre otras en el software Cooja para la simulación de los casos de estudios. Finalmente se realiza la implementación de un servidor MQTT y la integración con Node-red a fin de presentar un ejemplo de lectura y escritura en diferentes tópicos de un broker, asi como la verificación y tránsito de datos. Con este estudio se entrega una metodología para la selección de la tecnología que más se adapta a cada tipo de cultivo.

Palabras Clave:

- **IoT**
- **NODO SENSOR**
- **PROTOCOLOS DE COMUNICACIÓN**
- **AGRICULTURA INTELIGENTE**

Abstract

The development of smart agriculture has presented extensive development in recent years, that is why countless proposals have been presented around the world. This high variability of technologies used in the implementation of this type of solutions has generated certain users depending on what types of equipment or communication protocols to use depending on the application case. In this article, the different jobs and technologies used in IoT applied to agriculture are analyzed, comparing their technical characteristics through documentary analysis, simulations of case studies, among others. After this study, the results obtained from the bibliographic and documentary review are described by means of tables, in addition sensor nodes are reproduced with specific technical characteristics such as their communication protocol, energy consumption, degrees of protection of the devices, security of the implemented networks, among others in the Cooja software for the simulation of the case studies. Finally, the implementation of an MQTT server and the integration with Node-red are carried out in order to present an example of reading and writing in different topics of a broker, as well as the verification and data transit. This study provides a methodology for selecting the technology that best suits each type of crop.

Key words:

- **IoT**
- **SENSOR NODE**
- **COMUNICATION PROTOCOL**
- **INTELLIGENT AGRICULTURE**

Capítulo I

1. Planteamiento del problema de investigación

1.1. Introducción

La tendencia del Internet de las cosas (IoT), ha desencadenado un constante desarrollo de nuevas maneras de utilizar la interconexión en la búsqueda de ayudar a las personas mejorando su calidad de vida, generando un impulso en la búsqueda de mayor eficiencia en gestión de recursos y una reducción de costo (Verdouw, 2016). Las empresas, ciudades y diversos sectores productivos, así como el sector agrícola implementan cada vez más soluciones de IoT. Este rápido crecimiento también presenta desafíos como: Integración de millones de dispositivos de diversos proveedores que utilizan aplicaciones personalizadas, integración de cosas nuevas a la infraestructura de red ya existentes, protección de los dispositivos nuevos configurados con diversos niveles de seguridad. El sector agrícola tiene varios retos que superar de cara al futuro, se lo considera como un sector primario y de vital importancia para la provisión de alimentos y otros productos de primera necesidad (Deepa, 2021). El IoT tiene un papel preponderante para que este sector pueda avanzar y adaptarse a los cambios y demanda que se avecinan en el futuro (Yan, Yan, Ke, & Tan, 2016).

El IoT se es una herramienta potencial para optimizar el proceso de cultivar la tierra mediante el monitoreo, el almacenamiento de datos y la evaluación automatizada, buscando aumentar el rendimiento de los cultivos y reducir el impacto ambiental (Abbasi, Yaghmaee, & Rahnama, 2019). Estudios relacionados coinciden en que la valoración del IoT se realiza en función del análisis de los datos recopilados de las cosas, el desarrollo de sensores de bajo consumo y bajo costo permite recopilar un conjunto de datos ambientales y enviarlos a través de medios inalámbricos a una base de datos, los cuales pueden someterse a un análisis abstracto o un análisis a profundidad (Guerrero, Estrada-González, Medina-tejeda, Rivera-Gutierrez, & Alcaraz-Aguirre, 2017); así la agricultura moderna busca

transformar a la agricultura tradicional en una agricultura inteligente, con optimización de recursos y mejora de calidad, de esta manera la tecnología IoT se sitúa como un enfoque prometedor para lograr estos cometido. (Khattab, Abdelgawad, & Yelmarthi, 2016). La aplicación más común de utilización de nodos sensores en el monitoreo de los campos de cultivo se enfoca en el análisis de datos ambientales principalmente la temperatura, humedad, e indicadores de la calidad de suelo como el PH, niveles de nutrientes, entre otros, que se consideran como factores importantes en la toma de decisiones para la obtención de cultivos y cosechas saludables (Khattab, Abdelgawad, & Yelmarthi, 2016). Se han desarrollado sistemas óptimos de riego agrícola mediante redes de nodos sensores y manejo de datos a través de teléfonos inteligentes y aplicaciones web, con lo que se consigue que el contenido de humedad del suelo se mantenga de manera apropiada para el crecimiento de vegetales, reduciendo costos y aumentando la productividad agrícola (Muangprathub, y otros, 467-474) (Mekala & P. Viswanathan, 2017). Por otra parte, también existen propuestas de sistemas de detección de plagas mediante la aplicación de sensores inalámbricos que adquieren y transmiten imágenes hacia una estación anfitriona remota, este sistema se limita a la detección y no propone ningún método de control de pestes (Priya, Praveen, & Srividya, 2013). Adicionalmente se han desarrollado trabajos que apoyan la toma de decisiones en función de modelos conceptuales de apoyo en la agricultura inteligente mediante una red de sensores de adquisición de datos y gestión de tareas (Chiluisa, Lagla, Rivas, & Alvarez, 2021). Gracias a la globalización tecnológica se implementan y desarrollan proyectos de agricultura inteligente en Ecuador, cuya diversidad geográfica es un factor positivo para la práctica agrícola, que representa el principal ingreso de las comunidades rurales. En Cañar, se desarrolló una arquitectura que permite a la comunidad de agricultores: monitorear, administrar y manejar información de las variables de clima y suelo que inciden en el crecimiento del cultivo de maíz, con el objetivo de ayudar

en la toma de decisiones óptimas y oportunas basadas en la información presentada mediante gráficos estadísticos (Sichiqui, y otros, 2019).

Considerando el cacao como uno de los principales productos de exportación nacional se realizó el diseño de una arquitectura IoT de bajo costo basado en la tecnología Wireless sensor network (WSN) para monitoreo agrícola en cultivos de cacao, la información adquirida favorece la gestión sostenible del cultivo mediante la correcta administración de recursos, facilitando el control de calidad del producto y la prevención de planes de protección contra plagas y enfermedades (Guillermo, García, Rivas, Huerta, & Clotet, 2018).

Dentro de la optimización de recursos se puede mencionar el diseño de un motor de reglas y procesador de eventos complejos en el contexto de IoT para la agricultura de precisión el cual realiza un análisis prescriptivo que consiste no solo en predecir o detectar patrones de eventos, sino en tomar decisiones automáticas. La evaluación de este proyecto fue realizada vía simulación y los resultados arrojados demuestran la viabilidad de utilizar el sistema en infraestructuras de bajo coste para pequeños y grandes productores (Karim, Karim, & Frihida, 2017). Con lo que se ha podido evidenciar se han realizado un sin número de proyectos relacionados sobre estos temas, pero se puede identificar que en cada proyecto utilizan distintas tecnologías en el momento de implementar la experimentación.

Con tal variabilidad en el desarrollo de proyectos relacionados a la agricultura inteligente es importante buscar qué tipo de tecnología usar dependiendo de las condiciones propias del cultivo. Además de poder orientar a los productores al uso de estas tecnologías sin profundizar en temáticas como el Big Data, inteligencia artificial (IA), protocolos de comunicación, entre otros, es decir se debe buscar la aplicación del IoT como una herramienta a capitalizar para hacer uso de los datos digitalizados en la toma de decisiones, estimaciones y proyecciones, evitando tener demasiados datos, pero poca información. Con lo antes detallado se puede afirmar que existe una gran variabilidad de

tendencias en esta área y que no existe una guía objetiva que facilite a los usuarios la selección de componentes adecuados para sus proyectos. La presente investigación se centra en las aplicaciones de IoT desarrolladas en favor de la agricultura, considerando el avance tecnológico y su masificación como la base de conexión de sensores, actuadores y otras tecnologías inteligentes con el fin de lograr la migración hacia la agricultura de precisión, teniendo en cuenta que debido a la incursión del IoT en la agricultura, los procesos y procedimientos tradicionales han sido modificados. El presente trabajo se convertirá en una herramienta que permita contrarrestar las infraestructuras probadas, para el futuro desarrollo e implementación de proyectos relacionados con la tecnificación agrícola. El análisis de las soluciones implementadas, permitirá distinguir con claridad las potencialidades que cada uno de los nodos sensores, equipos de comunicación y protocolos presentan para la resolución de problemas concretos, en un área específica, permitiendo incrementar la eficiencia en el diseño y dimensionamiento de proyectos, además se ofrece alternativas en los proyectos que ya se encuentran operando, para perfeccionarlos de acuerdo a las diferentes condiciones y necesidades presentes en el sector agrícola.

1.2. Justificación

La investigación, se enfocará en analizar nodos sensores, equipos y protocolos de comunicación que han sido utilizados en la agricultura inteligente, ya que, debido a la incursión del internet de las cosas en la agricultura, los procesos y procedimientos tradicionales han sido modificados. El presente trabajo se convertirá en una herramienta que permita contrarrestar las infraestructuras probadas, para el futuro desarrollo e implementación de proyectos relacionados con la tecnificación agrícola.

El análisis de las soluciones implementadas, permitirá distinguir con claridad las potencialidades que cada uno de los nodos sensores, equipos de comunicación y protocolos presentan para la resolución de problemas concretos, en un área específica. Esto permitirá

aumentar la eficiencia en el diseño y dimensionamiento de proyectos, además ofrecerá mejores alternativas en los proyectos que ya se encuentran trabajando, para perfeccionarlos de acuerdo a las diferentes condiciones y necesidades presentes en el sector agrícola.

El desarrollo de proyectos de IoT aplicado en la agricultura, difundirá los beneficios a las zonas rurales al permitir la innovación, mejora en la producción y optimización de recursos agrícolas, además de contribuir con el acceso a servicios básicos e indispensables como la educación y la salud.

El documento presenta el resultado de una investigación de carácter documental, así como la evaluación en base a simulaciones de nodos sensores y protocolos de comunicación aplicados en la agricultura inteligente, características, estándares, velocidades de transmisión, número de dispositivos interconectados, seguridad en la comunicación y la descripción general del proyecto en el que fueron aplicados en favor de la agricultura. El método se fundamenta en el análisis sistemático del área, con el fin de constituir una herramienta, útil para promover proyectos de innovación y transferencia tecnológica.

1.3. Hipótesis de investigación

El análisis de nodos sensores y protocolos de comunicación aplicados en la agricultura inteligente contribuye en el diseño y dimensionamiento de proyectos relacionados con la tecnificación agrícola.

1.4. Antecedentes

Los factores que intervienen en el crecimiento de las plantas ocupan un lugar muy importante en la explotación agrícola, entre estos cabe mencionar: climáticos, bióticos (técnica o manejo), edáficos (estructura del suelo). Cada uno de estos factores comprende

varios subfactores. La acción de ellos sobre los rendimientos es interdependiente y el hombre tiene la capacidad de controlar o modificar su acción. (Hernández et al., 2019).

Es importante conocer el comportamiento de las variables meteorológicas para hacer un uso sustentable de los recursos de la naturaleza, es necesario entonces evaluar y diseñar sistemas inalámbricos de monitoreo y la utilización de sistemas embebidos, de tal forma que pueda llegar a ser implementada en la población de agricultores, brindando una herramienta tecnológica que permita adquirir, adecuar, y transmitir la información de la monitorización de variables ambientales tales como la temperatura ambiente, humedad relativa y humedad del suelo a una estación base, donde los usuarios puedan acceder remotamente para visualizar y analizar la información de los datos recopilados en la red, actualmente a esta tecnología se la conoce como internet de las cosas (IoT).

Los profesionales del área tecnológica, involucrados en la implementación del IoT en la agricultura deberán analizar todas las variables y características propias del entorno para aplicar la arquitectura más adecuada. Jose Perez, manifiesta que el trabajo parte de la identificación de la relevancia del paradigma IoT en el presente y futuro, a partir del enriquecimiento de las condiciones de cada persona y su entorno, para luego dar los conceptos del mismo. (Pérez, Mendoza, & M., 2019)

Por lo cual se hace posible tasar el impacto económico de IoT por año antes de 2025 en la agricultura, que se enmarca en un uso dentro de las fábricas como “mejora del campo de la agricultura” con un valor aproximado de 1 trillón de dólares y hasta un 60% de reducción de pérdidas, con lo que se puede deducir que una gran parte de la producción agrícola tendrá como objetivo la migración hacia la denominada agricultura de precisión. (Manyika, y otros, 2017)

La presente investigación formará parte del proyecto “Sistemas de alerta temprana para heladas en las Provincias de Cotopaxi y Tungurahua” el cual se ejecuta en la Universidad de las Fuerzas Armadas ESPE en coordinación con el CONGOPE. Adicionalmente los resultados obtenidos darán soporte al proyecto PLAGRI el cual pretende la búsqueda de la integración de tecnologías de adquisición, transmisión y almacenamiento de datos en entornos agrícolas y es desarrollado por la Universidad de las Fuerzas Armadas ESPE y la Universidad Politécnica Salesiana. Mencionados proyectos cuentan con el respaldo del grupo de investigación Wicom Energy.

1.5. Objetivos

1.5.1. Objetivo general del proyecto

Efectuar una evaluación sistemática de los nodos sensores y los protocolos de comunicación más utilizados en la agricultura inteligente a través de simulaciones de redes IoT.

1.5.2. Objetivos específicos del proyecto

- Establecer las principales diferencias de consumo energético, anchos de banda, velocidad de transmisión, alcance y topologías de red entre los nodos sensores IoT aplicados a la agricultura inteligente, mediante el análisis de proyectos desarrollados, para definir los sistemas compatibles en función de la zona de estudio.
- Identificar las vulnerabilidades presentes en los protocolos de comunicación utilizados en IoT, para precautelar la información que se genera en la agricultura inteligente.
- Determinar las potencialidades de los nodos sensores y protocolos de comunicación aplicados en la agricultura inteligente, mediante un análisis de proyectos desarrollados y la simulación en software especializado, para brindar una herramienta que facilite el diseño y dimensionamiento de proyectos de tecnificación agrícola.
- Aplicar paquetes informáticos de simulación de IoT, para evaluar los nodos sensores y protocolos de comunicación más utilizados en la agricultura inteligente.

Capítulo II

2. Marco teórico

2.1. Introducción

La tecnología actual ha permitido que las empresas y sectores productivos innoven su enfoque para interactuar con la sociedad. Los usuarios se sienten más cómodos con la tecnología digital y utilizan dispositivos inteligentes para su beneficio. Las empresas proporcionan todos sus servicios o parte de ellos en línea. Desde la comodidad del hogar se puede comparar alimentos en línea, reservar viajes, realizar pedidos de ropa y mantenerse conectado con sus amigos y familiares.

Los hogares inteligentes pueden contar con sensores de movimiento, sensores de agua, luz, temperatura, etc. Puede existir sensores en los semáforos, transporte público, garajes, cámaras de seguridad, trenes, aviones. Todos estos sensores y dispositivos de medición recopilan y transmiten sus propios datos. Los datos pueden almacenarse y analizarse en una fecha posterior o pueden ser analizados de forma inmediata y ser utilizados para modificar ciertos parámetros o ejecutar acciones de control en procesos de cualquier tipo. La combinación de métodos, infraestructura, equipos, elementos e instrumentos utilizados en la tendencia expuesta converge para dar paso al Internet de las cosas o IoT. En la tabla 1 se revisa algunos ejemplos de la aplicación de la recopilación y análisis de datos a través de herramientas de IoT.

Tabla 1.

Ejemplos de aplicación de la recopilación y análisis de datos.

INSTITUCIÓN	APLICACIÓN
Empresas	Determinar patrones de compra

INSTITUCIÓN	APLICACIÓN
	Pronóstico de tendencias Optimización de la producción
Gobiernos Nacionales	Pronosticar tendencias de la población. Planificación de servicios de seguro social. Tasa de delitos.
Gobiernos Locales	Control de tráfico. Monitoreo de estacionamiento y garajes públicos. Asistencia de instituciones de emergencia. Gestión de residuos.

2.2. Internet de las cosas

El Internet de las cosas (IoT) se encuentra en evolución por lo cual no existe una definición estandarizada, por lo que varias instituciones o autores han propuesto su conceptualización sobre este tema según sus diferentes criterios y puntos de visa, a continuación, mencionaremos los más relevantes.

El IoT es una red de dispositivos físicos conectados de forma inteligente con la capacidad de recolectar datos del ambiente, en el cual interactúan las cosas, las comunicaciones, y las aplicaciones, y para realizar un análisis de datos recolectados. Un concepto más amplio define a IoT como una infraestructura de red global, dinámica y autónoma, en la cual, interactúan hardware y software (cosas físicas y virtuales), con un alto grado de autonomía de captura de datos, transferencia de eventos, conectividad de red e interoperabilidad. (Rueda & Portocarrero, 2017)

El RFID group define la IoT como: “La red mundial de objetos interconectados direccionables basado exclusivamente en estándares de protocolos de comunicación”, mientras que para el Cluster of European Research Projects: “En la IoT se espera que “las cosas” conviertan a los participantes activos en procesos sociales, de información y negocios en donde “estas cosas” sean capaces de interactuar y comunicarse entre ellos mismos y con el ambiente a través del intercambio de datos e información detectada a su alrededor, mientras reaccionan automáticamente a los eventos del “mundo físico/real” y son influenciados a través de procesos en ejecución que disparan acciones y crean servicios con o sin la intervención directa del ser humano”. (Gubbi, Buyya, Marusic, & Palaniswami, 2013)

Los diversos criterios sobre el concepto de IoT concuerdan en que las redes de comunicaciones son uno de los pilares fundamentales del IoT, permiten conectar dispositivos, máquinas, sensores o “cosas” que generan datos desde cualquier punto geográfico del planeta.

Cuando se habla de un proyecto de IoT no necesariamente se hace referencia a miles de sensores conectados a la vez; básicamente dos “generadores de datos”, que no se encuentren próximos y que dispongan de una red de comunicaciones para transmitir datos a Internet para su posterior tratamiento, ya se tendría la base para un proyecto de Internet de las cosas.

Un sistema de IoT generalmente se compone de sensores que monitorean eventos, accionadores que influencian el entorno, hardware que crea plataformas y conexiones, y software que proporciona un marco de trabajo para ejecutar procesos. En todas las etapas de creación de un sistema de IoT, deben tenerse en cuenta los problemas relacionados con la seguridad y la privacidad considerando que cada nivel de conectividad tiene distintos requisitos e inquietudes.

2.2.1. Tecnologías de Comunicación Para IoT

Las redes de comunicaciones han ido evolucionando hacia el sector del IoT, actualmente ha despertado el interés y la inversión de numerosas empresas. Los principios para una red de comunicación de IoT son:

- Bajas velocidades de datos.
- Baja frecuencia de transmisión.
- Movilidad y servicios de localización.
- Conexiones bidireccionales seguras.
- Bajo consumo de energía.
- Largo alcance de comunicación.

A continuación, se describe algunas de las redes de comunicación más utilizadas para la ejecución de proyectos de IoT.

2.2.2. Machine to machine GSM/GPRS

Las redes de comunicaciones a través del sistema M2M (Machine to Machine) han sido la principal apuesta por IoT por parte de las grandes empresas del sector de las telecomunicaciones. Siempre vinculadas a la tarjeta SIM, la conectividad por M2M ha nacido del modelo de negocio del GPRS y el pago por Mbyte transmitido, tal como tecnologías 3G/4G.

Sin embargo, el enfoque de un proyecto de IoT (conectar miles de dispositivos que manden pocos datos) es el principal enemigo del M2M por su difícil escalabilidad, cobertura asociada a un operador y coste vs datos transmitidos. Por otro lado, el alto coste energético que suponen las transmisiones de datos en tecnología 3G y 4G conlleva un problema a

menudo inasumible en equipos que deben ser desplegados en campo y alimentados por batería.

2.2.3. SigFOX

Es la red de comunicaciones LPWAN (Low-power Wide-area network) específica para IoT más extendida a nivel mundial, con una cobertura próxima al 98% del territorio Europeo y Americano. La red de Sigfox está construida sobre una modulación ultra narrow band (UNB) y opera en la banda de 868MHz en Europa y en la banda de 902MHz en Estados Unidos.

Uno de los principales motivos para el uso de Sigfox a día de hoy, aparte de tener un despliegue y cobertura casi global, es que los fabricantes de dispositivos IoT se han adaptado a su tecnología y facilitan la subida de datos a la nube de Sigfox quedando disponibles en los servidores de la compañía para su acceso a través de cualquier conexión a Internet. A esto hay que añadir el soporte disponible por Azure de Microsoft, lo que acelera en gran medida la ejecución de un proyecto de IoT. (Aldahdouh, Darabkh, & Al-Sit, 2019)

El bajo coste de esta tecnología, su aceptación por los fabricantes de dispositivos, o el que sea una red bidireccional son otros factores a favor. Por el contrario, al ser una frecuencia no licenciada podría encontrarse en un futuro fuera de mercado, ya que esta frecuencia podría ser regulada por los organismos públicos y adquirida por el sector de las grandes empresas de telecomunicaciones, las cuales quieran apostar por M2M o NB IoT.

2.2.4. LoRa

Es una red LPWAN con un modelo de negocio muy similar a Sigfox aunque con una tecnología algo diferente ya que, entre otras cosas, utiliza un espectro de comunicaciones un poco más amplio que SigFox. Una diferencia considerable es que LoRa es una red LPWAN

mejor preparada para una comunicación bidireccional en tiempo real con el dispositivo de IoT. Asimismo, las especificaciones para los fabricantes que quieran comunicar sus equipos a través de LoRa son más abiertas o menos estrictas que con Sigfox.

Por otro lado, la cobertura de LoRa es mucho menor que la de Sigfox, ya que actualmente solo se encuentra desplegada en Francia, Bélgica, Suiza, Países Bajos y Sudáfrica, factor sin duda determinante a la hora de plantear un proyecto de IoT. (Mekki K. , Bajic, Chaxel, & Meyer, 2018)

2.2.5. NarrowBand IoT

Es otra red con tecnología LPWAN, en este caso, la gran apuesta de las operadoras de telecomunicaciones a nivel global. Esta tecnología tiene su factor diferencial en que su espectro de funcionamiento está en el rango del LTE o 4G, por lo que su despliegue y explotación comercial está casi asegurada gracias a la red actualmente desplegada. No obstante, el despliegue de la red, la puesta en marcha de esta tecnología y las bondades de la misma están pendientes de ser analizadas por los expertos y por los propios clientes. (Mekki K. , Bajic, Chaxel, & Meyer, 197-202)

2.2.6. Bluetooth Low Energy

BLE o Bluetooth de baja energía (conocido también por Bluetooth ULP Ultra Low Power o Bluetooth Smart) es otra tecnología inalámbrica de comunicaciones al servicio de determinados sectores de aplicación dentro de IoT. Permite interoperar pequeños dispositivos desarrollados para usar Bluetooth y destinados a mandar paquetes de datos reducidos, en comparación con el resto de tecnologías que están capacitadas para mandar grandes volúmenes de datos.

El BLE está siendo la tecnología utilizada para dispositivos pequeños (aquellos que usan como batería una pila de botón), para dar servicios de señalización y localización de dispositivos, y que pueden durar meses gracias a la baja tasa de transmisión de datos que presentan. (Rahman & Chakraborty, 2018)

El BLE sin duda tiene su punto de entrada comercial a través de los dispositivos beacons, o balizas de localización, que están siendo utilizadas con otros objetivos dentro del marketing o de la localización de activos.

Sin duda la tecnología BLE será clave para el desarrollo de proyectos IoT para equipos o electrónica de consumo, como los electrodomésticos que se tiene en casa. Sin embargo, el corto alcance de los dispositivos y la necesidad de establecimiento de redes punto a punto a través de emparejamiento lo convierten en un protocolo de reducida utilidad en entornos industriales y redes de sensores.

2.2.7. Zigbee

Es una tecnología inalámbrica, muy utilizada desde hace años y centrada en aplicaciones domóticas e industriales. Actualmente los perfiles ZigBee PRO y ZigBee Remote Control (RF4CE) cumplen con las especificaciones de tasas de envío de datos bajas, pero con un alcance de cobertura cercano a los 100 metros. Éste es un aspecto fundamental y que supone descartar las comunicaciones por ZigBee en caso de proyectos donde los dispositivos a comunicar se encuentren muy alejados del concentrador de los datos.

Entre sus principales ventajas se pueden mencionar: bajo consumo, seguridad superior al resto de tecnologías, robustez, alta escalabilidad y capacidad para soportar un gran número de nodos. (Rahman & Chakraborty, 2018)

2.3. Protocolos de Comunicación Para IoT

2.3.1. Message Queue Telemetry Transport

El Internet de las cosas proporciona conectividad avanzada de servicios, dispositivos y sistemas que van por encima de las asociaciones de máquina a máquina (M2M) e incluye una gama de aplicaciones, protocolos y dominios. La simplicidad de MQTT código fuente abierto hacen que este protocolo sea adecuado para entornos como el IoT. (Soni & Makwana, 2017).

MQTT es uno de los protocolos de comunicación M2M más antiguos, que se introdujo en 1999. Fue desarrollado por Andy Stanford-Clark de IBM y Arlen Nipper de Arcom Control Systems Ltd (Eurotech). Es una mensajería de publicación/suscripción protocolo diseñado para comunicaciones M2M ligeras en redes restringidas. El cliente MQTT publica mensajes en un bróker MQTT, que están suscritos por otros clientes o puede conservarse para la futura **suscripción**. Cada mensaje se publica en una dirección, conocida como tema. Los clientes pueden suscribirse a múltiples temas y recibe cada mensaje publicado en cada tema. MQTT es un protocolo binario y normalmente requiere un encabezado fijo de 2 bytes con cargas útiles de mensajes hasta un tamaño máximo de 256 MB. Utiliza TCP como protocolo de transporte y TLS/SSL para la seguridad. Así la comunicación entre el cliente y el corredor es una conexión orientada. Posee tres niveles de Calidad de servicio (QoS) para la entrega fiable de mensajes. MQTT es más adecuado para grandes redes de dispositivos pequeños que debe ser monitoreado o controlado desde un servidor back-end en Internet. No está diseñado para la transferencia de dispositivo a dispositivo ni para datos de multidifusión a muchos receptores. Es un protocolo de mensajería que ofrece sólo unas pocas opciones de control. (Naik, 2017)

2.3.2. Constrained Application Protocol

Es un protocolo M2M ligero del IETF, CoAP admite solicitud / respuesta y recurso/observar (variante de publicación / suscripción). CoAP es principalmente desarrollado para interoperar con HTTP y la web RESTful a través de proxies simples. CoAP usa un Identificador Universal de recursos (URI) en lugar de temas. El editor publica datos en el URI y el suscriptor se suscribe a un recurso particular indicado por el URI. Cuando un editor publica nuevos datos en el URI, todos los suscriptores están notificados sobre el nuevo valor según lo indicado por el URI. CoAP es un protocolo binario y normalmente requiere un encabezado fijo de 4 bytes con pequeñas cargas de mensajes de hasta un tamaño máximo depende del servidor web o la tecnología de programación, utiliza UDP como protocolo de transporte y DTLS para seguridad. Por lo tanto, los clientes y servidores se comunican a través de datagramas sin conexión con menos fiabilidad. CoAP admite la negociación de contenido para expresar una representación preferida de un recurso; esto permite al cliente y servidor evolucionar independientemente, agregando nuevas representaciones sin afectarse el uno al otro. (Naik, 2017)

2.3.3. Advanced Message Queuing Protocol

Es un protocolo M2M ligero de mensajería corporativa, AMQP admite tanto solicitud/respuesta como publicación/suscripción. Ofrece una amplia gama de funciones relacionadas a la mensajería, como una cola confiable, mensajería de suscripción y publicación basada en temas, enrutamiento y transacciones flexibles. El sistema de comunicación AMQP requiere que el editor o el consumidor creen un "intercambio" con un nombre dado y luego transmite ese nombre. Los editores y los consumidores utilizan el nombre de este intercambio, un consumidor crea una "cola" y la adjunta. Los mensajes recibidos por el intercambio deben ser emparejados con la cola a través de un proceso llamado "enlace". AMQP intercambia mensajes de varias formas: directamente, en forma de

abanico, por tema o por encabezados y utiliza TCP como protocolo de transporte predeterminado y TLS / SSL y SASL para seguridad, la comunicación entre cliente y broker está orientado a la conexión. (Naik, 2017)

2.3.4. Simple/Streaming Text Oriented Messaging Protocol

Es un protocolo basado en texto similar a HTTP, STOMP proporciona un encabezado de mensaje conocido como "marco" similar a AMQP. Se lo puede denominar como el terreno intermedio entre AMPQ y MQTT, compatible con ActiveMQ, RabbitMQ, Gozirra, Sprinkle y muchos otros. Está diseñado para la comunicación asíncrona entre clientes a través de un mediador de mensajes, está basado en frames o comando (operación), un mensaje o body y unas cabeceras del mensaje o headers. Se compone de una serie de comandos para la interacción entre cliente e intermediario de mensajes, entre las cuales están: (Stavrev, Terzieva, & Golev, 2018)

- **connect:** Establece conexión con el broker de mensajería.
- **subscribe:** El cliente se suscribe a un destino del broker (una cola o un topic).
- **send:** El cliente envía un mensaje a un destino del broker (cola o topic).
- **disconnect:** Cierra la conexión con el broker de mensajería.

2.4. Arquitectura IoT

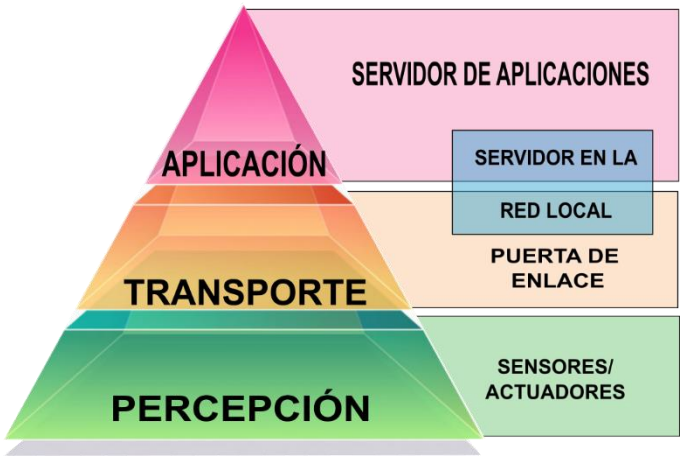
El conjunto de hardware y software de la tecnología IoT implementada, que agrupa a los sensores, transductores, actuadores, sistemas embebidos y diferentes sistemas de monitoreo comprenden la capa de precepción. Los datos recopilados se transmiten a través de una conexión cableada o una conexión inalámbrica hacia un controlador, el cual es responsable de recopilar datos de los sensores y proporcionar conectividad hacia la red o Internet, estos dispositivos y protocolos conforman la capa de transporte. Mientras que la capa de aplicación está conformada por los controladores y los sistemas experto que tienen

la capacidad de tomar decisiones inmediatas o de enviar datos a una computadora más potente para su análisis. Esta computadora más potente puede estar en la misma LAN que el controlador, o bien puede ser accesible únicamente por medio de una conexión a Internet.

Los elementos primarios de medida tales como equipos portátiles para entrenamiento físico, marcapasos implantados, medidores de aire en una mina y medidores de agua en el campo de un establecimiento agrícola, requieren conectividad inalámbrica y debido a que muchos sensores están "en el campo" son impulsados por baterías o paneles solares, por lo que se debe tener en cuenta el consumo de energía y utilizar opciones de conexión de baja potencia para optimizar y ampliar la disponibilidad del sensor. La figura 1 muestra una idea general de una arquitectura de IoT.

Figura 1.

Representación generalizada de una arquitectura de IoT.



2.4.1. Nodos Sensores

Los nodos sensores, son un conjunto de dispositivos autónomos, distribuidos físicamente en un área geográfica para monitorizar condiciones físicas o ambientales, con capacidad de almacenar y comunicar datos en una red, está compuesto por un procesador, una memoria, un transceptor, uno o más sensores, un conversor de señal análoga a digital

(ADC) y una fuente de alimentación. (Rueda & Portocarrero, 2017). La figura 1 muestra un modelo generalizado de los componentes de un nodo sensor.

Las características más relevantes de un nodo sensor son:

- Alcance de transmisión.
- Capacidad de procesamiento
- Capacidad de almacenamiento
- Suministro de energía.

2.4.2. Red de Sensores

La Unión Internacional de Telecomunicaciones (ITU-T), define una red de sensores como una red compuesta por nodos sensores interconectados, que intercambian datos detectados, usando comunicación inalámbrica o cableada. Estas redes de sensores están densamente desplegadas, ya sea dentro del ambiente donde ocurre un fenómeno o muy cerca de él, y se basan en el esfuerzo colaborativo de todos sus nodos para la obtención de los datos. (Rueda & Portocarrero, 2017)

2.4.3. IoT y Fog computing

La computación en la niebla más conocido como fog computing extiende el paradigma de cloud computing (computación en la nube) al borde de la red, permitiendo así una nueva generación de aplicaciones y servicios. (Bonomi, Milito, Zhu, & & Addepalli, 2012)

El Fog Computing tiene como objetivo acercar el procesamiento a los usuarios finales, evitando una explotación excesiva de los recursos de la nube, reduciendo aún más las cargas computacionales. (Guardo, Di Stefano, La Corte, Sapienza, & Scatà, 2018)

Las características definitorias de la niebla son: baja latencia y conocimiento de la ubicación, distribución geográfica amplia, movilidad, número muy grande de nodos, función predominante del acceso inalámbrico, fuerte presencia de aplicaciones de transmisión y en

tiempo real, heterogeneidad; características que hacen de fog computing la plataforma adecuada para una serie de servicios y aplicaciones de Internet de las cosas (IoT). (Bonomi, Milito, Zhu, & & Addepalli, 2012)

2.4.4. Seguridad en redes IoT

Técnicamente los datos generados no han cambiado a lo largo del tiempo, siguen siendo grupos de 1 y 0; sin embargo, lo que ha cambiado es la cantidad, el volumen, la variedad y la taza de transmisión de los datos generados.

En la actualidad, los datos recopilados adquieren nuevas características. El mundo digitalizado abrió las compuertas de la recopilación de datos. Los dispositivos de IoT con sensores habilitados recopilan más datos de carácter personal. Los dispositivos de medición de estado físico, los sistemas de supervisión residencial, cámaras de seguridad y las transacciones con tarjeta de débito son todos sistemas que recopilan datos personales, así como datos ambientales. Suelen combinarse datos de distintos orígenes y los usuarios pueden no tener conocimiento de ello. La combinación de los datos de monitoreo del estado físico, con los datos de monitoreo de la casa podrían generar puntos de datos para ayudar a rastrear los movimientos o la ubicación de un propietario. Este tipo de recopilación cambiante de datos y la agregación pueden utilizarse para fines positivos y contribuir al entorno, pero también aumenta la posibilidad de que se produzca una invasión de nuestra privacidad, robo de identidad y espionaje corporativo.

La información de identificación personal (PII, personally identifiable information) o la información confidencial (SPI, sensitive personal information) son datos sobre una persona viva que se pueden utilizar de forma individual o con otra información para identificar, contactar o localizar a una persona específica. Los datos recopilados de empresas e instituciones gubernamentales también pueden contener información confidencial con

respecto a secretos corporativos, patentes de productos nuevos o seguridad nacional. Algunos ejemplos de información de identificación personal son:

- Dirección de correo electrónico.
- Clasifciación crediticia.
- Número de tarjetas de débito / crédito
- Fecha de nacimiento.
- Nombre de usuarios/contraseñas.
- Dirección particular.
- Facturas de consumo.

Mientras que en datos informativos se puede citar:

- Valores de pluviómetro.
- Número de automóviles en uan intersección.
- Valores demográficos.
- Lectura de termómetro.
- Valores migratorios.
- Cultivos promedio por provincia.
- Próximo horario de unidades de transporte.

Debido a que se puede recopilar y almacenar cantidades exponenciales de datos confidenciales e informativos, ha aumentado la necesidad de contar con seguridad adicional para proteger esta información hackers y uso indebido.

Proteger la red incluye aplicar protocolos, tecnologías, dispositivos, herramientas y técnicas que protegen datos y mitigan las amenazas. Los estándares, procedimientos y políticas de seguridad deben respetarse en el diseño de todos los aspectos de la red. Esto debe incluir los cables, los datos en tránsito, los datos almacenados, los dispositivos de red y

los dispositivos terminales. La tabla 2 muestra algunas buenas prácticas de seguridad. (Cisco Networking Academy, 2021)

Tabla 2.

Buenas prácticas de seguridad de red.

Acción	Descripción
Definir políticas de seguridad	Delimitar claramente las reglas y tareas de la empresa u organización, tareas y expectativas.
Realizar evaluación de riesgos	Conocer el valor de lo que se protege ayuda a priorizar la inversión en seguridad
Seguridad de acceso físico	Restringir el acceso a armarios, racks de conexión y servidores. La seguridad informática inicia en la seguridad física.
Realizar copias de respaldo	Ejecutar y probar los respaldos.
Instalar los parches de seguridad y actualizaciones	Actualizar programas y sistemas operativos de servidores, redes y equipos de usuario final.
Incorporar equipos de protección de red	Utilizar routers y firewalls y otros dispositivos de seguridad de red.
Capacitar a los usuarios	Educar a usuarios, empleados y colaboradores sobre procedimientos seguros.

Los expertos y analistas en tecnología predicen un uso aún más expansivo de dispositivos y aplicaciones de IoT en el futuro, junto con dispositivos, servicios y aplicaciones en constante evolución que tocan el espacio de IoT, las organizaciones a menudo están ansiosas por aprovechar los beneficios comerciales. Sin embargo, muchas empresas tienen razón en ser cautelosas en su búsqueda de los beneficios de las soluciones de IoT debido a preocupaciones de seguridad de IoT muy reales. Las implementaciones de IoT plantean nuevos desafíos únicos de seguridad, privacidad y cumplimiento para las empresas de todo el mundo.

Mientras que la ciberseguridad de la información tradicional se basa en el software y cómo se implementa, la seguridad para IoT agrega una capa adicional de complejidad a medida que los enfoques físico y lógico convergen. Una amplia gama de escenarios operativos y de mantenimiento en el espacio de IoT se basan en la conectividad de dispositivos de un extremo a otro para permitir que los usuarios y los servicios interactúen, inicien sesión, solucionen problemas, envíen o reciban datos de los dispositivos. Las empresas desean aprovechar las eficiencias de IoT como el mantenimiento predictivo, por ejemplo; pero saber qué estándares de seguridad de IoT deben cumplir es esencial, porque la tecnología operativa (OT) es demasiado importante y valiosa para arriesgarse en caso de intrusiones, y otras amenazas.

Aunque los dispositivos de IoT pueden parecer demasiado pequeños o demasiado especializados para ser peligrosos, existe un riesgo real en lo que realmente son: computadoras de propósito general conectadas a la red que pueden ser secuestradas por atacantes, lo que genera problemas más allá de la seguridad de IoT. Incluso el dispositivo más básico puede volverse peligroso cuando se ve comprometido a través de Internet. Una vez que los atacantes tienen el control, pueden robar datos, interrumpir la prestación de servicios o cometer cualquier otro delito cibernético que cometan con una computadora.

Los ataques que comprometen la infraestructura de IoT infligen daños, no solo con violaciones de datos y operaciones poco confiables, sino también daños físicos a las instalaciones, o peor aún, a las personas que operan o dependen de esas instalaciones. (Azure, 2021).

2.4.5. Ventajas y Desventajas del IoT

Las aplicaciones de IoT están latentes en múltiples aspectos cotidianos, lo que refleja su importancia, entre las principales ventajas se puede citar:

- Realizar un seguimiento de intereses y necesidades de individuos, así como implementar bonificaciones de fidelidad a clientes.
- Las autoridades pueden evaluar requisitos de transporte y desarrollo vial en cada localidad.
- Optimizar recursos energéticos en hogares e industrias.
- Reducción de tiempos de inactividad en la producción mediante la predicción de los requisitos de mantenimiento.
- Análisis y proyección de variables medio ambientales.

Sin embargo, el hecho es que aún existen muchos desafíos y problemas relacionados con el uso de IoT, y no deben ser subestimados, dentro de sus desventajas cabe mencionar:

- Las empresas fabricantes de dispositivos portátiles y prestadoras de servicios acceden a mucha información personal de los usuarios.
- Una falla en la red puede traer consecuencias graves.
- Se incrementa la cantidad de correo no deseado.
- Probable reducción de empleo.
- Fuga de información.

2.5. Agricultura Inteligente

En la agricultura tradicional el proceso de cultivo se basa en la experiencia e intuición para realizar las distintas labores del campo siguiendo un calendario prefijado año tras año. Mientras que la aplicación de nuevas tecnologías de recopilación, almacenamiento y análisis de datos, en conjunto con los sistemas de información y comunicación se presentan como una alternativa que permite el monitoreo, estimación y control de parámetros relacionados con la productividad agrícola, este sistema en conjunto ha sido llamado agricultura de precisión o agricultura inteligente.

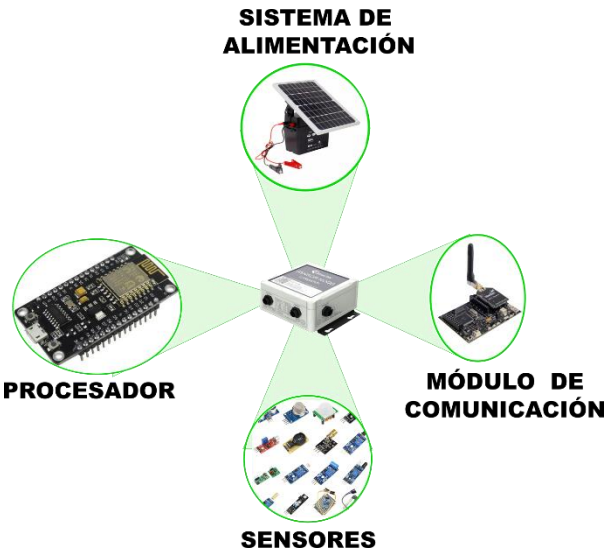
El cambio climático experimentado en los últimos años hace que la variabilidad del clima reduzca la eficiencia en la producción agrícola, es por eso que una de las áreas de mayor interés dentro de la agricultura inteligente es la meteorología, al usar sistemas con múltiples sensores para la monitorización en tiempo real de las condiciones climáticas, buscando obtener predicciones concisas y precisas. (Organización de las naciones unidas para la Alimentación y Agricultura, 2021)

La incorporación de sensores de alta precisión mejora la productividad agrícola ya que entre otras cosas permiten obtener datos objetivos de los cultivos para llevar un control del crecimiento de las plantas, prevenir pérdidas provocadas por circunstancias meteorológicas adversas o plagas y así facilitar el retorno de las inversiones.

El conjunto de elementos que permiten el monitoreo de variables físicas es también conocido como nodo sensor o estación de monitoreo y tiene una estructura generalizada que consta de: un sistema de alimentación, un procesador, un sistema de comunicación y el conjunto de sensores, estos últimos le pueden dar la característica de estación meteorológica, estación de suelo o una combinación de ambos. En la figura 2 se puede observar los bloques de una estación de monitoreo o nodo sensor.

Figura 2.

Principales componentes de una estación de monitoreo.



2.5.1. IoT en la Agricultura

En los últimos años, el uso de la tecnología en el sector agrícola ha tenido un fuerte impulso por parte de investigadores. El surgimiento del Internet de las Cosas (IoT) y su colaboración con otras tecnologías como el cómputo en la nube ha permitido procesar y analizar datos en tiempo real facilitando la toma de decisiones. (Guerrero, Estrada, Medina, & Rivera, 2017)

El uso de IoT en la agricultura se describe como una tecnología destinada a organizar la gran variedad de sensores para formar redes, a través de los cuales se puede recolectar información de tierras aptas para la agricultura y análisis en tiempo real de los resultados transmitidos a los agricultores para que puedan tomar las decisiones más adecuadas. (Pérez, Mendoza, & M., 2019)

La aplicación de IoT en agricultura encuentra un gran aliado por parte de la computación en la nube para el tratamiento de datos como: uso eficiente de los insumos

como fertilizantes y pesticidas, reducción de costos, control de ganado, agricultura de interiores, invernaderos y establos, piscicultura, monitoreo del almacenamiento en tanques de agua, tanques de combustible, silos, asignación de recursos a demanda sin límite, mantenimiento y actualizaciones realizadas en Back-end, fácil y rápido desarrollo incluyendo la colaboración con otros sistemas en la nube. (Patil, Al-Gaadi, Biradar, & Rangaswamy, 2012)

2.5.2. Beneficios de IoT en la Agricultura

En la agricultura inteligente mediante la tecnología IoT se puede obtener información sobre: el clima, humedad, temperatura, fertilidad del suelo, los agricultores pueden conocer el estado de sus cultivos en cualquier momento y desde cualquier lugar. (Gómez, Real, Morán, Grijalva, & Recalde, 2019)

En términos generales se puede describir los siguientes beneficios de la aplicación del IoT dentro de la agricultura inteligente:

- Agricultura comunitaria en zonas urbanas y rurales aprovechando hardware y recursos de software y grandes cantidades de datos.
- Trazabilidad logística y cualitativa de la producción de alimentos que permite reducir costos y el desperdicio de insumos mediante el uso de datos en tiempo real para la toma de decisiones.
- Generación de modelos de negocio en el contexto agrícola que permitan establecer una relación directa con el consumidor.
- Monitoreo de cultivos que permite reducir costos y el robo de maquinaria.
- Sistemas de riego automático que funcionan de acuerdo con la temperatura, humedad relativa, humedad del suelo que se obtienen a través de sensores.
- Recolección automática de parámetros ambientales a través de redes de sensores para posterior procesamiento y análisis.

- Sistemas de soporte de decisiones que analizan grandes cantidades de datos para mejorar el funcionamiento eficiencia y productividad.

Algunos proyectos utilizan cámaras inalámbricas juntamente con drones para apoyar las tareas de monitoreo del cultivo en tiempo real; así como apps para informar a los agricultores sobre las condiciones actuales de su cultivo. Otras tecnologías destacadas que se combinan con IoT para desarrollar soluciones agrícolas son: las redes inalámbricas de sensores, la nube informática.

El IoT es un pilar en el desarrollo tecnológico y se convertirá en una herramienta importante en la resolución de problemas en el contexto agrícola. Por esta razón, se realiza una revisión de la literatura con el objetivo de identificar diferentes nodos sensores y protocolos de comunicación de IoT en la agricultura.

2.6. Componentes Comerciales Aplicados en la Agricultura Inteligente

El futuro de la agricultura se basa en el monitoreo de datos en tiempo real, los equipos de detección en el campo y el análisis de datos a largo plazo, esto ha desencadenado disputas entre diferentes empresas y organizaciones que buscan una ventaja tecnológica por lo que han desarrollado diversos equipos, instrumentos y soluciones completas en este campo. A continuación, se citan ejemplos de estas tecnologías.

2.6.1. IoT Gateway Ethernet / MQTT – Converter HD67930-B2

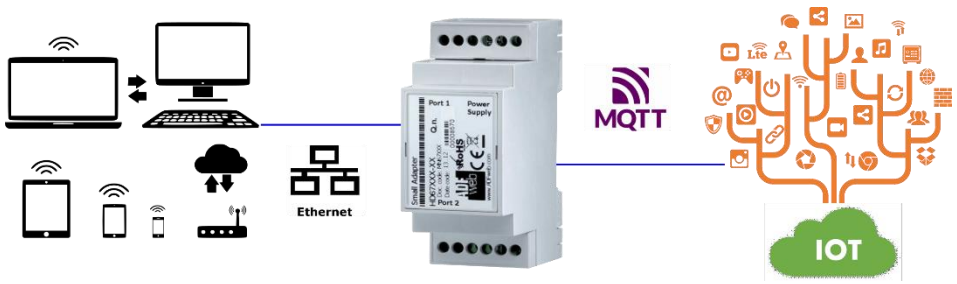
Es un dispositivo que permite publicar los datos recibidos de Ethernet (mensajes TCP / UDP) en un servidor MQTT, brindan un acceso rápido y fácil al mundo del IoT, son compatibles con Servidores IoT que funcionen con el protocolo MQTT. La figura 3 muestra un esquema de la aplicación del Gateway.

La comunicación MQTT puede cifrarse mediante los protocolos TLS / SSL,

garantizando así una comunicación segura y protegida, además los mensajes y comandos son completamente configurables por lo que es posible interactuar con otros dispositivos y/o software basados en Ethernet. (ADF, 2017)

Figura 3.

Representación de la aplicación del Gateway Ethernet/MQTT.



2.6.2. Envira

La empresa desarrolla soluciones Smart Agro para monitorizar granjas agrícolas y ganaderas innovadoras, las cuales incorporan todo tipo de sensores para adaptarse a las necesidades de cada cliente. En la figura 4 se muestra una representación de una arquitectura Envira.

2.6.3. Nanoenvi AG

Los dispositivos Nanoenvi® AG permiten crear redes de sensores inalámbricos para monitorizar, predecir y optimizar la gestión de los recursos agrícolas en tiempo real gracias a su conexión a la nube. Incorporan 6 conectores para la conexión de sensores, tanto analógicos como digitales, es compatible con diversos tipos de sensores: meteorológicos (temperatura, humedad, presión, lluvia, radiación solar), gases (H2S, CO, CO2, SO2, etc.) o agrícolas (humedad de la hoja, PH del suelo, dendrómetros, etc).

2.6.4. *Monitorización Meteorológica en Agricultura de Precisión*

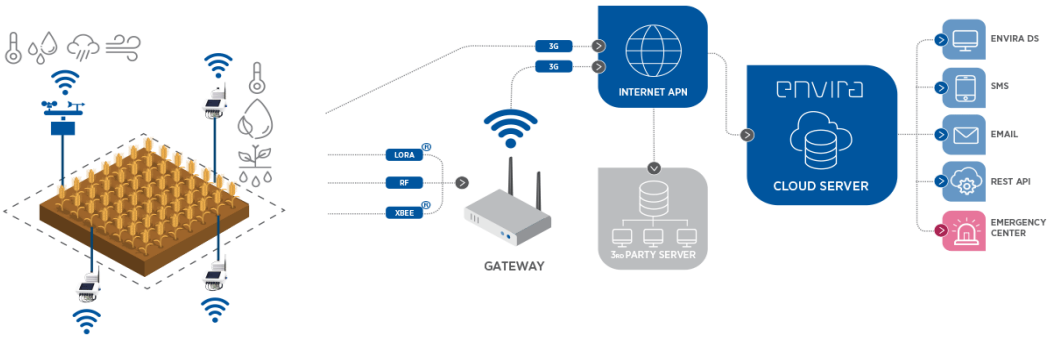
El sistema está formado por una red de sensores que captura variables relevantes sobre la climatología a través de estaciones agroclimáticas y un sistema informático inteligente para la explotación de los datos climáticos capturados con el fin de generar alertas y notificaciones ante situaciones que afecten a los cultivos. Integra sistemas de monitorización meteorológica como:

- Dirección y velocidad del viento.
- Temperatura
- Humedad
- Radiación solar
- Radiación UV
- Radiación PAR
- Pluviometría
- Presión barométrica

Adicionalmente se puede instalar cualquier otro sensor de medidas atmosféricas que se precise. Todos estos sensores se integran con los sistemas de gestión de datos de ENVIRA IoT. Las comunicaciones se realizan de forma inalámbrica a través de tecnologías como 3g, 4G, LORA® y próximamente Narrow-Band. (Envira, 2018)

Figura 4.

Representación de una arquitectura Envira.



2.6.5. Monnit

Brinda una opción en el monitoreo de cultivos mediante el Internet de las cosas (IoT), sus sensores tienen prestaciones como las alertas por mensaje de texto, correo electrónico o llamada. Y una amplia variedad de alrededor de más de 80 tipos de sensores, la figura 5 muestra una representación general de la arquitectura Monnit. (Monnit, s.f.).

2.6.6. Sensor inalámbrico de humedad (RH) ALTA

El sensor de humedad (RH) inalámbrico ALTA mide la humedad relativa en el dispositivo. El sensor regresa Valores de humedad relativa y temperatura al iMonnit Online (sistema de notificación y monitoreo de sensores). El sistema calcula el punto de rocío a partir de los datos y almacena los tres puntos de datos en el sistema en línea donde los datos pueden ser revisado y exportado como hoja de datos o gráfico. Las notificaciones se pueden configurar a través del sistema en línea para alertar al usuario cuando se han definido umbrales cumplido o superado.

2.6.7. Sensor de velocidad de aire inalámbrico

El sensor de velocidad del aire inalámbrico ALTA mide la diferencia de presión entre dos puertos de entrada, la temperatura y la altitud determina la velocidad a la que se mueve el aire en un sistema y transmite la medición a iMonnit.

- Rango de medición: -50 m / sa 50 m / s
- Calibrado y compensado por temperatura

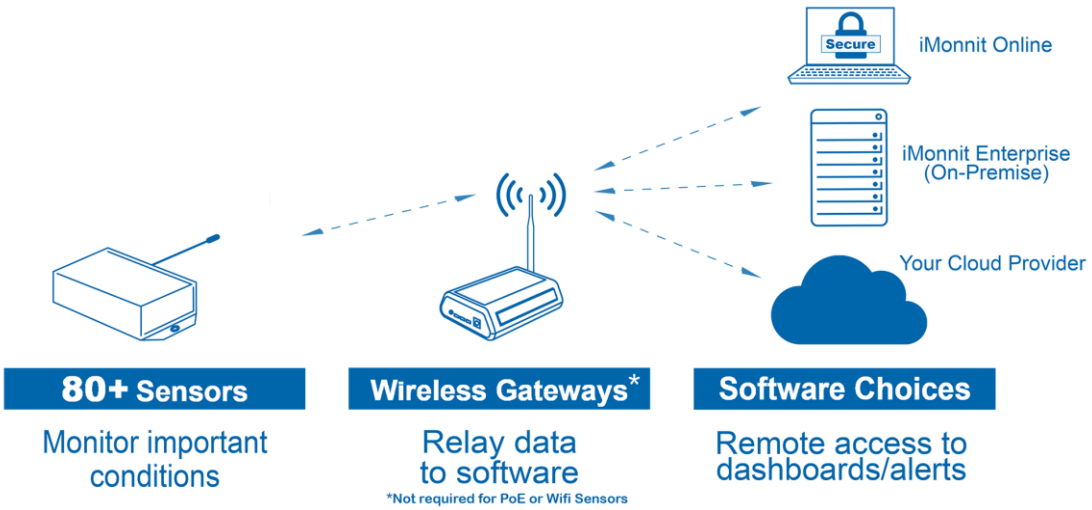
2.6.8. Sensor inalámbrico de humedad del suelo

El sensor de humedad del suelo ALTA mide la humedad, tensión y temperatura del suelo, usa un elemento de matriz granular resistivo para medir con precisión el potencial hídrico mátrico (tensión de humedad del suelo) y un elemento de temperatura basado en termistor. Entre sus principales características están:

- Seguro de usar tanto en temperaturas cálidas como heladas.
- Lecturas de humedad en centibar.
- 0 a 240 centibar.
- No se disuelve en el suelo.
- Compensado internamente por la salinidad que se encuentra comúnmente niveles.
- Fácil de instalar y usar en comparación con los tradicionales tensiómetros
- Electrodos de acero inoxidable.
- No requiere mantenimiento.
- Lecturas de temperatura en C / F.
- Cable extraíble de 5 pies.

Figura 5.

Representación de una arquitectura Monnit.



2.6.9. Libelium

Diseña y fabrica soluciones tecnológicas para hacer posible Internet de las cosas, está evolucionando desde un negocio de fabricación de hardware con el objetivo de convertirse en un proveedor completo de soluciones de IoT. Son los fabricantes de waspmote uno de los nodos sensores más utilizados, además tienen una amplia gama de soluciones IoT tales como: agua, agricultura, ambiente, estacionamiento, industria, rastreo, turmismo, e-salud. La figura 6 muestra una representación de los componentes de Libelium. (Libelium, 2021)

2.6.10. Plug & Sense

Es la versión encapsulada de Waspmote. Esta línea permite el fácil despliegue de las redes de Internet de las cosas de forma escalable. La plataforma consta de un robusto encapsulado impermeable con enchufes externos específicos para conectar los sensores, el panel solar, la antena e incluso el cable USB para reprogramar el nodo, especialmente

diseñado para ser escalable, fácil de implementar y mantener, sus principales características son:

- Configuración sencilla, permite agregar o cambiar una sonda de sensor en segundos.
- Carcasa robusta a prueba de agua IP65.
- Opción de panel externo con energía solar.
- Radios disponibles: 802.15.4, Zigbee, 868 MHz, 900 MHz, WiFi, 4G, Sigfox y LoRaWAN.
- Programación por aire (OTAP) de varios nodos a la vez (a través de WiFi o radios 4G).
- Interfaz gráfica e intuitiva.
- Acelerómetro integrado de 3 ejes.
- Protocolos industriales opcionales: RS-485, Modbus, CAN Bus.
- Módulo de batería externa opcional.
- Conector SIM externo para los modelos 4G.
- Totalmente certificado: CE (Europa), FCC (EE. UU.), IC (Canadá), ANATEL (Brasil), RCM (Australia), PTCRB (EE. UU., Conectividad celular), AT&T (EE. UU., Conectividad celular

2.6.11. Smart Environment PRO

Permite el cálculo del índice de calidad del aire (AQI), gracias a los sensores de gas electroquímicos que proporcionan valores de ppm extremadamente precisos y un sensor de partículas de alta gama.

- Monóxido de carbono (CO) (concentraciones bajas).
- Dióxido de carbono (CO_2).
- Oxígeno molecular (O_2).
- Ozono (O_3).

- Óxido nítrico (NO) (concentraciones bajas).
- Dióxido nítrico (NO_2).
- Dióxido de azufre (SO_2) (alta precisión).
- Amoníaco (NH_3) (concentraciones altas y bajas).
- Metano (CH_4) y otros gases combustibles
- Sulfuro de hidrógeno (H_2S).
- Materia de partículas (PM1 / PM2.5 / PM10) - Sensor de polvo
- Temperatura
- Humedad
- Presión atmosférica
- Luminosidad (precisión de luxes) para iluminación inteligente
- Ultrasonido (medición de distancia)

2.6.12. Smart Agriculture Xtreme

Es una evolución de la línea de agricultura con una nueva selección de sensores profesionales de alta gama. Permite monitorear múltiples parámetros ambientales que involucran una amplia gama de aplicaciones, desde el análisis de crecimiento de plantas hasta la observación del clima. Hay sensores para el monitoreo atmosférico y del suelo y la salud de las plantas. (Libelium, 2020)

- Medición de temperatura de superficie sin contacto SI-411.
- Temperatura de las hojas y los botones florales SF-421.
- Nivel de oxígeno del suelo SO-411.
- Radiación solar (onda corta, PAR y UV): SP-510, SQ-110 y SU-100.
- Temperatura, humedad y presión del aire.
- Contenido volumétrico de agua y temperatura del suelo TEROS 11.

- Conductividad, contenido de agua y temperatura del suelo TEROS 12.
- Potencial hídrico del suelo TEROS 21.
- Presión de vapor, humedad, temperatura y presión atmosférica en el suelo y el aire VP-4.
- Humedad de las hojas Phytos 31.
- Diámetro del tronco, tallo y fruto: DC3, DD-S y DF.
- Estaciones meteorológicas avanzadas.
- Luminosidad (precisión de luxes).
- Ultrasonido (medición de distancia).
- Tipo 4-20 mA (entrada genérica).
- Tipo RS-232 (entrada genérica).

Figura 6. *Representación de componentes Libelium.*

2.6.13. Lain Holding

Presenta al mercado una variedad de equipos, sensores y posibilidades orientados a la gestión de cultivos. La figura 7 muestra los componentes de la arquitectura; a continuación, se detalla algunas de estas.

2.6.14. Estación Meteorológica

Es capaz de medir 12 variables climáticas que incluyen: temperatura del aire, humedad, relativa, presión de vapor, presión barométrica, velocidad del viento, ráfaga y dirección, radiación solar, precipitación, contador de rayos y distancia.

2.6.15. Sensor de humedad de hojas

Este sensor de humedad de hojas LWS está estandarizado, calibrado y diseñado para detectar la humedad (presencia y duración) y la formación de hielo desde el primer momento. Algunas de su s aplicaciones son: predecir cuándo rociar los cultivos, cuantificar el almacenamiento de agua en el dosel de la planta, en el estudio y monitoreo de cultivos para enfermedades foliares, incluyendo roya y tizón.

2.6.16. Indicador de lluvia y precipitación

Consta de un dispositivo basculante de vaciado automático patentado, con buenas características de precisión y confiabilidad que lo hacen apto para su aplicación en el mercado de agricultura IOT. Su calibración es manual y garantiza una precisión de +/- 2%.

2.6.17. Sonda de humedad del suelo de capacitancia

Esta sonda de humedad del suelo debajo de la superficie ofrece medición de la humedad del suelo basada en capacitancia. Presenta una longitud de sonda de 800 mm y 6 sensores de humedad del suelo y 6 sensores de temperatura del suelo. Se puede usar para pastos u otras aplicaciones de medición bajo la superficie.

2.6.18. Agricultura IOT inteligente XT: Sensores integrados

Es una solución mejorada y ampliada que incluye muchos sensores profesionales de alta gama, que permiten realizar el monitoreo de múltiples parámetros ambientales que involucran una amplia gama de aplicaciones, desde análisis de crecimiento de plantas hasta

observación del clima. Se pueden conectar hasta 32 sensores dentro de los cuales se puede mencionar: (Lain Holding, 2021)

- Medición de temperatura de superficie sin contacto SI-411.
- Temperatura de brotes de hojas y flores SF-421.
- Nivel de oxígeno en el suelo SO-411.
- Radiación solar (onda corta, PAR y UV): SP-510, SQ-110 y SU-100.
- Temperatura del aire, humedad y presión.
- Conductividad, contenido de agua y temperatura del suelo GS3.
- Conductividad, contenido de agua y temperatura del suelo 5TE.
- Temperatura del suelo y contenido volumétrico de agua 5TM.
- Potencial de agua del suelo MPS-6.
- Presión de vapor, humedad, temperatura y presión atmosférica en suelo y aire VP-4.
- Humedad foliar Phytos 31.
- Diámetro del tronco, tallo y fruto: DC2, DD-S y DF.

Figura 7.

Representación de componentes de la arquitectura Lain.

2.7. Análisis de herramientas de simulación para IoT

Las herramientas de simulación son utilizadas para representar y evaluar el comportamiento de un equipo o sistema en un tiempo determinado, permiten realizar una evaluación antes de ejecutar la implementación definitiva.

La aplicación de herramientas de simulación en el IoT comprende la afirmación de ejecución, confiabilidad, estimación de consumo energético, convergencia de redes. Se basan en la reconstrucción de modelos donde cada dispositivo tiene sus propias necesidades de diseño, lo que genera cierto grado de dificultad en la recreación de elementos, por lo cual existen muy pocos sistemas de simulación de fácil acceso.

Seleccionar la herramienta adecuada para la reconstrucción de IoT es una tarea difícil, por lo que se debe tener claro el enfoque y qué parámetros son los que se necesitan evaluar. A continuación, se realiza una breve descripción de algunas herramientas de simulación IoT. (Manivannan & Radhakrishnan, 2020)

Iotify es un simulador de IoT en la nube, permite simular instalaciones de IOT a gran escala en su propio laboratorio virtual. El tráfico personalizable con lo que se evalúa la plataforma en cuanto a escala, seguridad y fiabilidad para identificar y solucionar problemas; analizar cómo la latencia de la red afecta al rendimiento general del sistema antes de implementar la arquitectura final.

Matlab y Simulink, pueden ser utilizados en diseño, prototipo y despliegue de aplicaciones IoT tales como mantenimiento predictivo, optimización de operaciones, control de supervisión, etc.

Permite acceder a streaming de datos y datos archivados y realizar el preprocesamiento mediante las interfaces integradas para almacenamiento en la nube,

bases de datos relacionales y no relacionales y protocolos tales como REST, MQTT y OPC UA. Además, es posible diseñar algoritmos y análisis de IoT personalizados de forma rápida a partir de miles de funciones prediseñadas de probada eficacia para ámbitos como la limpieza de datos, machine learning/deep learning, visión artificial, controles y optimización. (Mathworks, 2021)

Bevywise IoT es una herramienta de simulación para decenas de miles de clientes MQTT, el cual permite desarrollar, probar y demostrar sus servidores y administradores de IoT. Se puede ejecutar pruebas a partir de creación de plantillas para sus dispositivos físicos. Mediante la herramienta de creación masiva es posible simular miles de dispositivos virtuales únicos con temas y mensajes únicos. Las redes simuladas se pueden almacenar en la base de datos MySQL y reutilizarlas cuando sea necesario. (Bevywise, 2021)

Ansys hace posible la creación de los sistemas que alimentan el IIoT (Industrial Internet of things) y luego usar los datos del IIoT para crear gemelos digitales de activos físicos que nos permitan comprender mejor los sistemas, predecir problemas y fallas, optimizar procesos y mejorar el tiempo y los costos de producción.

Para garantizar un desarrollo rentable y oportuno, la ingeniería exitosa de los productos IIoT se basa en aplicaciones como: el diseño y la ubicación de antenas, el desarrollo de sistemas de paquetes de chips, la electrónica de potencia, la interferencia / compatibilidad electromagnética (EMI / EMC), la confiabilidad de la electrónica y la simulación de baterías. (ANSYS, 2021).

Cooja, el sistema operativo Contiki incluye un potente simulador de red llamado Cooja. Permite simular nodos que ejecutan aplicaciones Contiki y que se organizan en una red de sensores inalámbricos. Cooja brinda la posibilidad de emular cada nodo a nivel hardware para poder observar de manera más precisa su comportamiento a la vez que

facilita la comunicación con otros nodos que pertenecen a la misma red. (Fraga Castro, 2015).

Las principales características de este simulador son las siguientes:

- Diseñado para sistemas embebidos con poca memoria o recursos.
- El núcleo gestiona eventos, que pueden ser ordenado dinámicamente en tiempo de ejecución.
- Permite utilizar varios protocolos de comunicación, entre los que se destacan IPv6 y 6LoWPAN
- Pueden instalarse sobre una gran variedad de dispositivos
- Está escrito en C.

2.8. Análisis Bibliométrico

La bibliometría se define como la aplicación de métodos matemáticos y estadísticos para analizar la trayectoria de la comunicación escrita o literatura científica, así como a los autores que la producen. Los instrumentos utilizados para este análisis son conocidos como indicadores bibliométricos los cuales proporcionan información sobre los resultados de la actividad científica en cualquiera de sus manifestaciones. Mediante estos indicadores se puede determinar el crecimiento de cualquier área científica teniendo en cuenta parámetros como: cantidad de artículos publicados, colaboración de autores, centros de investigación, países, producción de científicos, entre otros. (Escorcia Otalora, 2008)

2.8.1. VOSviewer

Es una herramienta de software para construir y visualizar redes bibliométricas que incluyen revistas, investigadores o publicaciones individuales. También ofrece una funcionalidad de minería de textos que puede utilizarse para construir y visualizar redes de

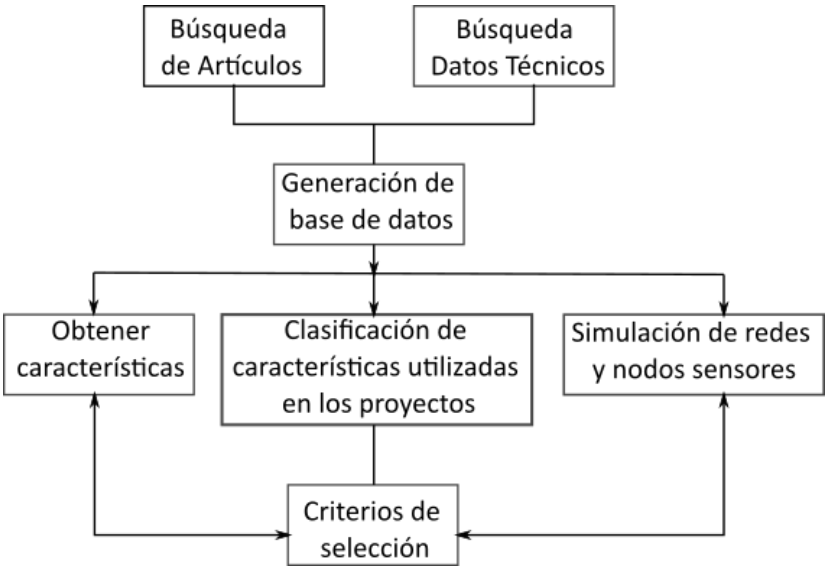
coocurrencia de términos importantes extraídos de un cuerpo de literatura científica. Los elementos de las redes pueden estar conectados por enlaces de co-autoría, co-ocurrencia, citación, acoplamiento bibliográfico o co-citación y se puede aplicar a diferentes bases de datos como Web of Science, Scopus, Dimensions, PubMed, RIS, o Crossref JSON. (VOSviewer, 2021)

2.9. Metodología de la Investigación

La investigación se centra en la descripción de cuatro características relevantes: consumo energético, grados de protección de los dispositivos, seguridad de las redes implementadas y la simulación de nodos sensores y protocolos aplicados en la agricultura inteligente como una herramienta de análisis de rendimiento de la red, en la figura 8, se describe el procedimiento realizado para sintetizar la información registrada.

Figura 8.

Procedimiento de síntesis de información.



Para la búsqueda de documentos se utilizó la base de datos de scopus y google schoolar, de las cuales mediante la cadena de búsqueda IoT AND agriculture se obtiene 1785

artículos, posteriormente se realiza una selección de investigaciones recientes, considerando los artículos a partir del año 2015. Otros criterios de selección incluyen la utilización de nodos sensores la descripción de protocolos utilizados y consumo energético; los artículos que describen claramente su arquitectura fueron considerados como artículos referentes de soluciones de IoT aplicados a la agricultura inteligente. En caso de no tener ninguna de las restricciones mencionadas anteriormente, la cantidad de artículos sería demasiado amplia y fuera del alcance de esta investigación. Además, se busca presentar las características de consumo energético de los elementos microcontroladores y sistemas de transmisión citados en los artículos en los cuales no se precisa el consumo promedio del proyecto implementado. Para lo cual se realiza la búsqueda en páginas de los fabricantes, así como en trabajos relacionados sobre características de modos de operación y consumo energético de los elementos y sistemas antes mencionados.

Con la finalidad de elaborar esta herramienta se aplicaron tres experimentos, el primero consiste en análisis bibliométrico con la herramienta VOSviewer a través de la cual se obtiene los resultados de búsquedas de palabras claves. El segundo experimento consiste en el análisis documental a través de la cual se realiza la extracción de las características que son objeto de análisis en la presente investigación. En el tercer experimento, a través de la simulación se intenta exponer las principales herramientas que se dispone para la evaluación de proyectos, donde se implementan las características comunes detectados en este estudio. Finalmente se realizó la escritura de los diferentes apartados que componen el presente trabajo de investigación.

3. Experimentación y Resultados

3.1. Análisis bibliométrico

El primer experimento consiste en el análisis bibliométrico cuyos resultados son descritos a continuación: en la figura 9 se puede ver el crecimiento que se ha tenido en los últimos años en cuanto a la investigación del IoT en la Agricultura inteligente (IoT + Smart Agriculture), mientras que la figura 10 muestra la concentración de publicaciones por territorios en donde India destaca en la investigación en el área, para la construcción de esta información se utilizó la base de datos de Scopus y la cadena de búsqueda mencionada.

Figura 9.

Número de publicaciones por años SCOPUS (IoT + Smart Agriculture).

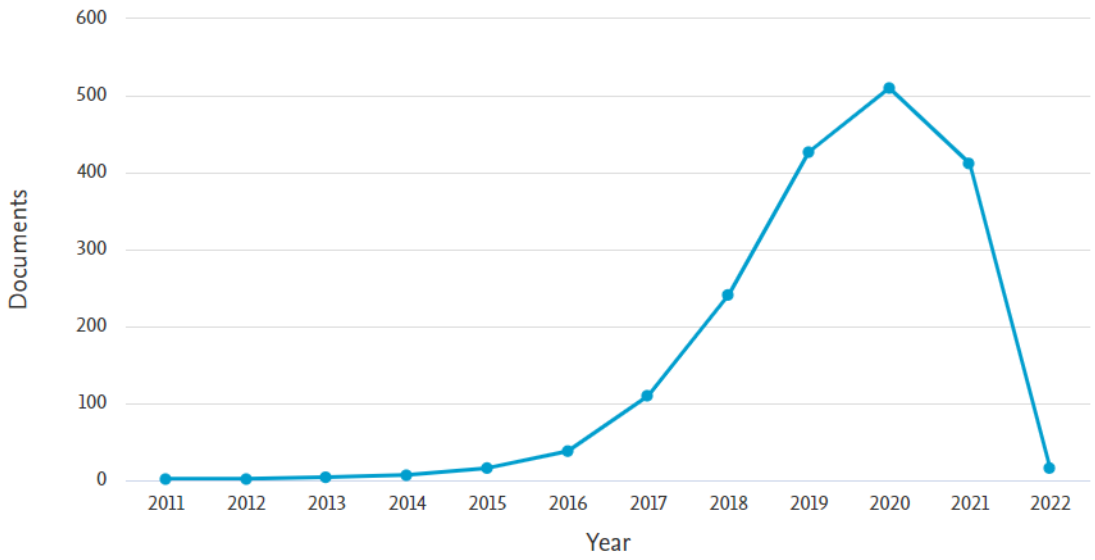
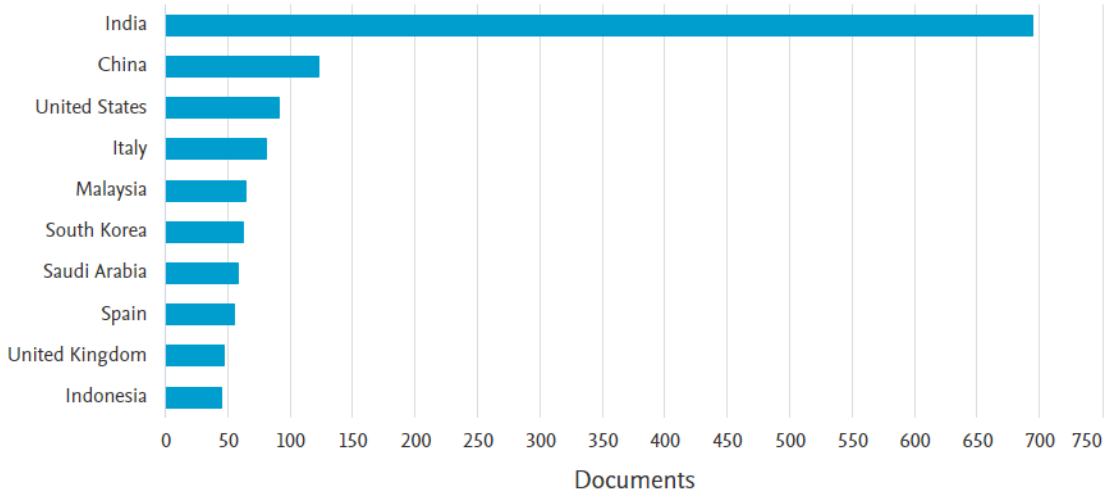


Figura 10.

Concentración de publicaciones por territorio.



Mediante la herramienta VOSviewer se realiza un análisis de conteo correlacionado de los términos asociados a IoT y la agricultura inteligente de un total de 1785 documentos, la figura 11 muestra una visualización de red, en la que los términos están representados por un color y por su etiqueta, el tamaño de la etiqueta está determinado por el peso (número de enlaces) del término. Cuanto mayor sea el peso de un término, mayor será la etiqueta y el color define el grupo al cual pertenece el término. Las líneas entre términos representan vínculos, mientras que la distancia entre términos en la figura indica la relación de co-citas. En general, cuanto más cerca están los dos términos, más fuerte es su relación.

Otra herramienta de análisis que se aplica en VOSviewer es el análisis de superposición, en la cual se aplica de forma similar los criterios descritos en la visualización de red, excepto los colores de cada término, los cuales pueden ser modificados en función de otras características como el año de publicación, promedio de citas, entre otras, en la figura 12 se muestra una representación de los enlaces de cada término y el promedio de su año de publicación, el color azul representa los más antiguos mientras que el rojo representa el promedio de publicación más reciente.

Figura 11.

Visualización de red de términos asociados a IoT y agricultura inteligente.

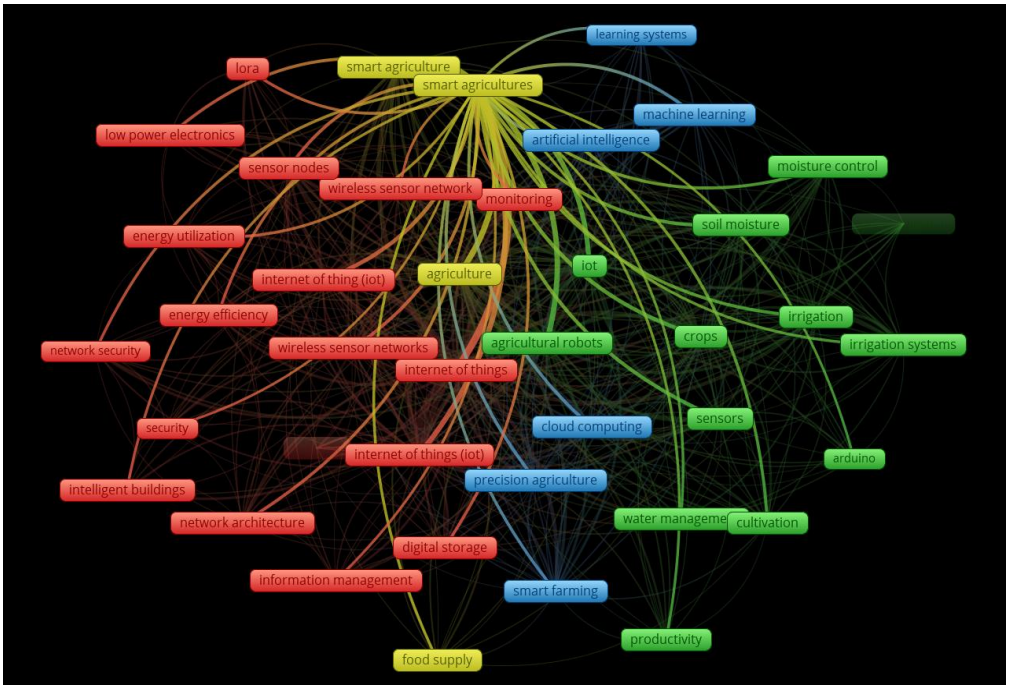
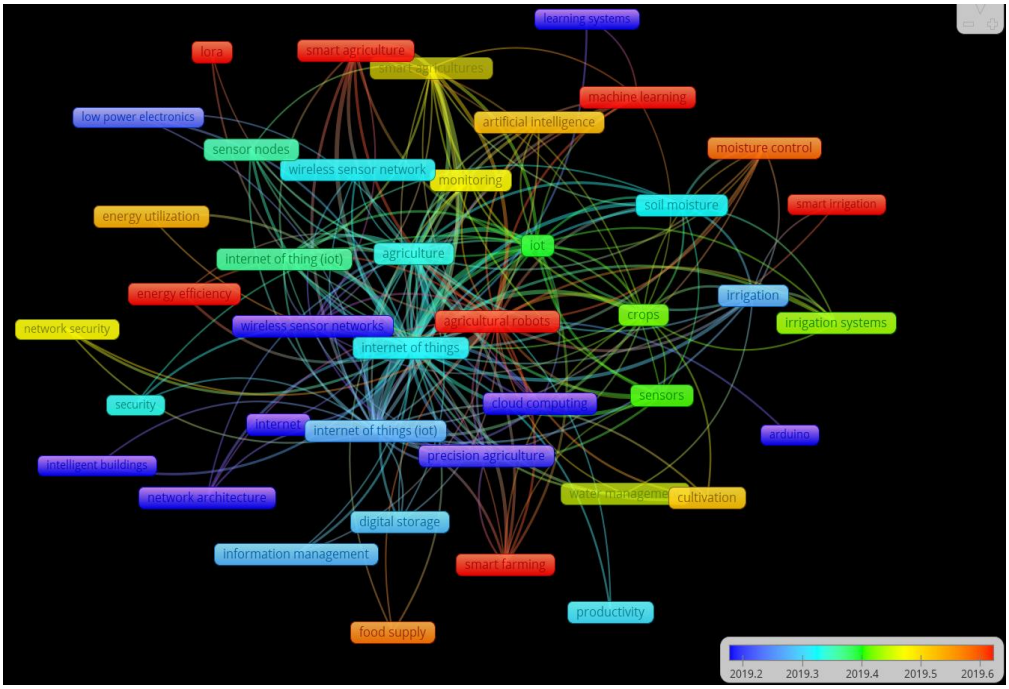


Figura 12.

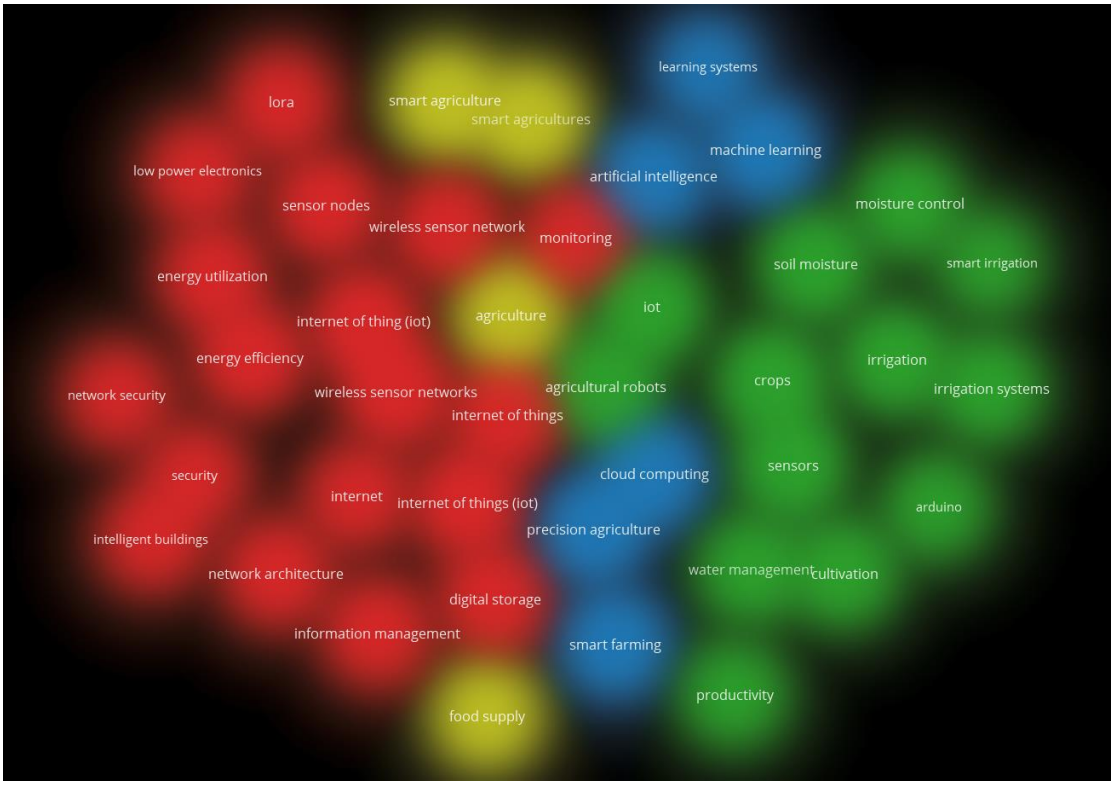
Visualización de superposición de términos asociados a IoT y agricultura inteligente.



Adicionalmente se puede aplicar el análisis de densidad de clústeres o grupos, los clústeres son definidos por medio de la técnica propia de VOS e incluye un número mínimo de términos, cada grupo se representa con un color distinto y el peso que se le da al color de un cierto clúster está determinado por el número de elementos que le pertenecen. La figura 13 muestra el análisis de densidad de los términos y cadena de búsqueda en cuestión, en la que se puede identificar 4 grupos y homogeneidad en el número de enlaces de cada termino.

Figura 13.

Visualización de densidad de clústers asociados a IoT y agricultura inteligente.



En las imágenes mostradas se tiene un total de 41 términos asociados con la cadena de búsqueda “IoT + Smart Agriculture”, agrupados en 4 clústers, con un total de 762 enlaces entre sí, a través de estos datos se define las áreas de interés y se procede al análisis

documental, para lo cual se realiza la selección de los artículos y extracción de información para la presentación, comparación y análisis de los datos obtenidos.

3.2. Análisis del consumo energético

En cuanto al consumo energético de los nodos sensores las investigaciones señalan que se busca que los dispositivos inalámbricos sean de bajo consumo de energía y que no requieran un alto flujo de datos. El bajo consumo de energía es importante, porque el tiempo de vida de un sistema de IoT, está ligado directamente al tiempo de autonomía de sus nodos sensores. Debido a que la energía disponible en la batería de un nodo sensor es un recurso agotable, es importante el estudio de la dinámica del consumo de la energía en los nodos sensores, con el fin de buscar una gestión óptima del recurso energético. (Amarillo & M, 2014)

Se debe considerar que el envío y recepción de datos desde un nodo sensor es una combinación de consumo de potencia de diferentes elementos. En la mayoría de casos, se han incorporado sistemas de recolección de energías alternativas que han perimido aumentar el tiempo de autonomía de la batería, generando un proceso de carga constante. Es necesario tomar en cuenta cada elemento responsable del consumo de energía para calcular la eficiencia energética y la vida útil de la batería. Una de las soluciones implementadas y ampliamente difundida es la aplicación de los diferentes modos de operación de las tarjetas controladoras, lo que permite disminuir el consumo cuando no se requiere realizar una transmisión de datos.

De manera general se puede considerar tres modos de trabajo: el modo de transmisión/recepción en el que los datos se transmiten/reciben utilizando el protocolo seleccionado; el modo activo donde ocurre el procesamiento, se forma el paquete de mensajes; finalmente el modo no activo o sleep constituye el modo de reposo o inactivo

durante el cual la mayoría de los periféricos del nodo sensor no están realizando ninguna tarea. La tabla 3 muestra ejemplos de consumo de energía de nodos sensores en sus modos de operación. (Heble S. , Kumar, Prasad, Samirana, & Rajalakshmi, 2018).

Tabla 3.

Ejemplos de nodos sensores y consumo energético.

Nodo Sensor	I Inactivo o sleep	I Activo	I transmisión
IITH	180 uA	11,58mA	26,58 mA
M33SS	200 mA	500 mA	600 mA
DZ50 SPS	3.3 uA	3.25 mA	26.5 mA
MicaZ SPS	170 uA	4.35 Ma	18.5 mA
TelosB PIS	13 uA	1.72 mA	19.12 mA
ECO	2 mA	3 mA	22 mA
Tiny Node	5 uA	3 mA	22 mA
Waspmote	7 uA	9 mA	20 mA
LOTUS	--	16 mA	17 mA
Sun SPOT	32 uA	206 mA	--
Tmote sky	5.1 uA	54.1 uA	195 mA

Otras investigaciones en las que se realiza la construcción de una arquitectura propietaria no especifican el consumo energético total, sin embargo, en función de los componentes descritos se puede realizar una estimación aproximada. La tabla 4 indica los consumos teóricos de tarjetas que han sido utilizadas en el desarrollo de prototipos.

Tabla 4.

Consumo energético de tarjetas controladoras utilizadas en IoT.

Controlador	I Activo	I Sleep
Arduino UNO	49 mA	34.5mA
Node MCU /ESP8266	15mA	10 uA
AT mega 328P	15 mA	0.36 mA

Los nodos sensores son dispositivos de energía restringida y, por lo tanto, algunos trabajos a más de analizar el consumo en el hardware han desarrollado protocolos que den un aporte al consumo eficiente de energía, con lo que se pretende prolongar la estabilidad de la vida útil de la arquitectura. Lo que se busca es un protocolo de agrupamiento distribuido para mejorar la eficiencia energética maximizando el área de cobertura considerando que enlace inalámbrico y la intensidad de la señal se ve muy afectada por las condiciones ambientales y no pueden considerarse parámetros de red ideales.

La tabla 5 muestra los tiempos estimados de duración de la batería, realizado por los diferentes autores, en base a la demanda individual de sus componentes.

Tabla 5.

Estimación de tiempo de vida de la batería de proyectos desarrollados.

Trabajo	Contribución Técnica	Estimación de Autonomía	Alimentación
(Borrero & Zabalo, 2020)	An Autonomous Wireless Device for Real-Time Monitoring of Water Needs	724 días	Li-Po 3.7V 2200mAh

Trabajo	Contribución Técnica	Estimación de Autonomía	Alimentación
(Heble S. , y otros, 2018)	A Low Power IoT Network for Smart Agriculture	243 dias	Li-Ion 2000mAh
(Riquelme, y otros, 2009)	Wireless Sensor Networks for Precision Horticulture in Southern Spain	223 días	AA NiMH 2700 mAh
(García-Fallas, 2016)	SESBeacon: Nodo Sensor Electrónico Para Alertas Tempranas	218 días	Li-Ion 3.6V 2250mAh
(Visconti, de Fazio, Velasquez, Del Valle Soto, & Giannoccaro, 2020)	Development of Sensors-Based Agri-Food Traceability System Remotely Managed by a Software Platform for Optimized Farm Management	168 días	Li-Po 4.1V 100mAh
(Ilie-Ablachim, Pătru, Florea , & Rosner, , 2016)	Monitoring Device for Culture Sub-strate Growth Parameters for Precision Agriculture: Acronym: MoniSen	183 días	2.4V 2400mAh (conv. elev. MCP1640)
(Zhao, Lin, Han, Xu, & Hou, 2017)	Design and Implementation of Smart Irrigation System Based on LoRa	12 días	3.6V 4800mAh
(López, y otros, 2015)	GAIA2: A Multifunctional Wireless De-vice for Enhancing Crop Management	1200 días	NiMH 4.8V 6000mAh
(Catelani, Ciani, Bartolini, Guidi, & Patrizi, 2020)	Characterization of a low-cost and low-power Environmental monitoring system	14 días	Li-Ion 7V, 3500 mAh,
(Estrada Mendoza, 2019)	Diseño de un nodo sensor para aplicaciones IoT		Li-Po 3.7V, 1000 mAh

Las tarjetas controladoras, así como los nodos sensores comerciales presentan diferentes modos de operación con el objetivo de optimizar el consumo energético y brindar mayor tiempo de autonomía a los sistemas; la incorporación de sistemas alternativos de carga de baterías, generalmente mediante paneles solares, es una tendencia marcada en los proyectos desarrollados.

3.3. Seguridad en los protocolos y arquitecturas de comunicación

Mantener una red segura garantiza la confianza de los usuarios de la red y protege sus intereses, por lo tanto, es necesario reconocer la velocidad y la escala a la que los adversarios están acumulando y refinando su potencial cibernético, los cibercriminales están llevando el malware a niveles de sofisticación e impacto sin precedentes, son expertos en el uso de técnicas de sigilo y evasión para ocultar su actividad, explotando brechas indefensas en la seguridad. A continuación, la tabla 6 presenta una breve descripción de algunos términos asociados a la seguridad de redes. (Cisco Networking Academy, 2021).

Tabla 6.

Descripción de términos asociados a la seguridad de redes.

TÉRMINOS DE SEGURIDAD	DESCRIPCIÓN
Activos	Es cualquier cosa de valor para la organización. Incluye personas, equipos, recursos y datos.
Vulnerabilidad	Es una debilidad en un sistema, o su diseño, que podría ser explotado por una amenaza.
Amenaza	Es un peligro potencial para los activos, los datos o la red de una empresa funcionalidad de enrutamiento.
Explotar	Es un mecanismo para tomar ventaja de una vulnerabilidad.
Mitigación	Es la contra medida que reduce la probabilidad o gravedad de una posible amenaza o riesgo. La seguridad de la red implica técnicas de mitigación múltiple.
Riesgo	Es la probabilidad de que una amenaza explote la vulnerabilidad de un activo, con el objetivo de afectar negativamente a una organización. Riesgo es medido

TÉRMINOS DE SEGURIDAD	DESCRIPCIÓN
	utilizando la probabilidad de ocurrencia de un evento y sus consecuencias.

Las amenazas a las que puede estar expuesta una arquitectura de IoT son diversas la tabla 7 describe algunos de los ataques que pueden presentarse y ejemplos de herramientas de mitigación, cabe mencionar que la combinación de dos o más herramientas es recomendable siempre que sea posible.

Tabla 7.

Ejemplos de ataques y acciones de mitigación.

Clasificación de la amenaza	Descripción	Herramienta de Mitigación
Suplantación de identidad	Un ataque por suplantación de identidad por IP es cuando un atacante/un tercero se hace pasar por una entidad distinta, pero de confianza, a través de falsificaciones de los datos ante una comunicación.	Autentificación de entidad par: Este servicio autentifica la fuente de una unidad de datos. La autentificación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autentificar la una o la otra.
Denegación de servicio	Dejar sin funcionar un equipo, impedir brindar un servicio o cortar la comunicación.	Control de acceso: Este servicio se utiliza para evitar

Clasificación de la amenaza	Descripción	Herramienta de Mitigación
		el uso no autorizado de recursos
Manipulación de información	Manipulación o remplazo de datos.	Integridad de datos: Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.
Divulgación de información	Proporcionar datos confidenciales a equipos o direcciones no autorizadas.	Confidencialidad de datos: Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.
Elevación de privilegios	Forzar a un dispositivo a ejecutar otras funciones a las cuales estaba restringido.	Control de acceso: Este mecanismo se utiliza para autentificar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a los recursos que posee.

A continuación, se aplica la metodología del análisis de conteo correlacionado de términos para seleccionar varios protocolos de comunicación los cuales han sido utilizados en soluciones de IoT aplicados a la agricultura inteligente (Chen, Miao, Hao, & Hwang, 2017) (Raza, Kulkarni, & Sooriyabandara, 2017). Generalmente estos protocolos son divididos según la distancia de transmisión, por ejemplo, Bluetooth (Singelée & Preneel, 2006), BLE (Tosi, Taffoni, Santacatterina, Sannino, & Fomica, 2017) e identificación por radio frecuencia (RFID) en corta distancia, Wi-Fi y ZigBee (Dignani, 2012) media distancia, mientras que las tecnologías de larga distancia se puede mencionar las redes celulares (4G) y las tecnologías conocidas como Low Power Wide Area Network o simplemente LPWAN dentro de las cuales se puede mencionar LoRA, NB-IoT y Sigfox. (Feng, Yan, & Liu, 2019), a continuación, se describen las aplicaciones y características de seguridad más relevantes de cada una de estas tecnologías:

3.3.1. Descripción de Seguridad de Zig Bee

Dadas las características de este protocolo, un mensaje puede ser recibido por cualquier dispositivo cercano. Esto es un inconveniente puesto que se puede incurrir en violaciones la privacidad de las personas, producir algún daño o inhabilitar algún sistema. ZigBee soporta el uso de protocolos estándar de encriptación y autenticación. En el diseño de la red debe considerarse el nivel de seguridad, complejidad y costo de los dispositivos considerando que el aumento de seguridad implica mayor capacidad de cómputo y memoria lo que conlleva un incremento de consumo energético. (Dignani, 2012). La autenticación de datos tiene por objeto garantizar que la información es válida y que no ocurrió ninguna adulteración, para ello el transmisor añade al mensaje un código especial conocido como MIC (Message Integrity Code). El MIC se genera con un método que conocen tanto el emisor como el receptor. Cuando recibe el mensaje el receptor calcula el MIC y si éste coincide con el que envía el transmisor, el mensaje se considera auténtico. El nivel de seguridad en el

control se incrementa con el número de bits del MIC. ZigBee soporta MIC de 32, 64 y 128 bits. La encriptación de un mensaje aporta con confidencialidad de la información. EL MIC en ZigBee se genera usando el protocolo CCM* (enhanced Counter with Cipher Block Chaining Message Authentication Code). El CCM* se usa en conjunción con AES (Advance Encryption Standard) de 128 bit y comparten la misma clave de seguridad, el uso de AES-CCM* logra autenticación y confidencialidad en el mensaje. (IMAGEN).

3.3.2. Descripción de Seguridad de Bluetooth

La tecnología Bluetooth se divide fundamentalmente en dos tipos de sistemas: Basic Rate (BR)/Enhanced Data Rate (DR) y Low Energy (LE). En el presente trabajo se describirá las características de seguridad de Bluetooth Low Energy o BLE debido a sus prestaciones para agricultura inteligente. (Sesé Vega, 2020).

BLE se caracteriza por implementar los mecanismos de seguridad en el host, además introduce dos nuevas funcionalidades a su modelo de seguridad: privacidad LE y firmado de datos: Privacidad LE, se basa en que los dispositivos modifiquen su dirección cada cierto tiempo mediante el uso de una clave llamada IRK (Identity Resolving Key), mientras que el firmado de datos se basa en el uso de una clave denominada CSRK (Connection Signature Resolving Key) compartida durante el proceso de pairing que se utiliza para firmar los datos y que el receptor pueda verificar su autenticidad en escenarios en los que el modo de seguridad activado no permita el cifrado. Existen actualmente dos clases de seguridad en BLE: LE Legacy Pairing y LE Secure Connections(V4.2). El uso de uno u otro modelo determina los mecanismos para la generación de claves, en ambos casos BLE utiliza el algoritmo AES-CCM para los servicios de cifrado y de integridad de mensajes.

3.3.3. Descripción de Seguridad de LoRa WAN

Las propiedades fundamentales que son compatibles con la seguridad LoRaWAN son: autenticación mutua, protección de la integridad y confidencialidad. La autenticación mutua se establece entre un dispositivo final LoRaWAN y la red, como parte del procedimiento de unión a la red. Esto asegura que solo los dispositivos genuinos y autorizados se unan a redes genuinas y auténticas, además el intercambio de mensajes LoRa WAN está autenticada en el origen, protegida contra reproducción y encriptada, esta combinación, garantiza que el tráfico de la red no se haya alterado, que provenga de un dispositivo legítimo, que no sea comprensible para los espías y que no haya sido capturado y reproducido por actores deshonestos. LoRaWAN es una de las pocas redes de IoT que implementa el cifrado de extremo a extremo (Lora Alliance, 2017). La información está encriptada por AES-CTR y lleva un contador de tramas (para evitar la repetición de paquetes) y un Código de integridad del mensaje (MIC) calculado con AES-CMAC (para evitar la manipulación de paquetes). AES se usa en el modo CTR estandarizado que hace uso de operaciones criptográficas XOR (como muchos otros modos como CBC5). Esto fortalece el algoritmo AES mediante el uso de una clave AES única para cada cifrado de bloque.

3.3.4. Descripción de Seguridad de NB IoT

Existen distintos métodos para gestionar la seguridad en una red de comunicaciones NB-IoT, entre los dispositivos y el servidor cloud donde se reporta la información. APN o plataforma de operador los operadores ofrecen para NB-IoT la posibilidad de que se monte un servidor intermedio que recoge los datos de la propia red de NB-IoT sin pasar por internet. La plataforma final del cliente va conectada típicamente mediante una conexión VPN segura con la plataforma del operador y esto hace que todo el camino desde el dispositivo hasta el servidor cloud del cliente sea seguro. Securización de protocolo UDP: en

este caso, los datos viajan encriptados de extremo a extremo por la misma tecnología, y es el servidor cloud quien se encarga de hacer la autenticación y la decodificación final de los datos. No aplicar seguridad es la posibilidad más fácil, pero no es recomendable. Esta opción se podría barajar solo en pruebas de funcionamiento, ya que en proyectos reales y de volumen se podrían recibir múltiples ataques sin capacidad alguna de hacerles frente.

La tabla 8 muestra características relevantes de los protocolos en cuestión.
Tabla 8.

Características de seguridad de protocolos utilizados.

Protocolo	Estándar	Autenticación	Encriptación	Alcance	Velocidad	Consumo Energético
BLE	IEEE 802.15.1	AES-CCM	AES-CCM	100m	1Mbps	10 mW
ZigBee	IEEE 802.15.4	AES-CCM	AES-CCM	100m	20, 40, 250 Kbps	36.9 mW
LoRa	IEEE 802.15.4g	AES-CTR	AES-CTR	Urbano 2Km, rural 15 Km	50 Kbps	100 mW
NB-IoT	3Gpp release 13	DTLS APN	DTLS APN	Urbano 1 – 8 Km Rural 25 Km	200 Kbps	106mW

Los autores de diferentes artículos coinciden en que la seguridad de la red radica básicamente en la integridad, autenticación y cifrado de datos, la figura 14 muestra el denominado triángulo de seguridad, cuyos componentes se recomienda tener en cuenta en el momento de diseñar una arquitectura IoT. Todas las tecnologías analizadas presentan protocolos que permiten incorporar estas seguridades. Es importante señalar que la incorporación de seguridades en la red demanda consumo de recursos informáticos lo que conlleva un mayor consumo energético por parte del nodo sensor. Los protocolos dejan abierta la posibilidad de establecer una red sin seguridades, lo cual no es recomendable bajo ningún punto de vista.

Figura 14.

Principales características de la seguridad de redes.

Los protocolos analizados tienen prestaciones de seguridad que incluyen encriptación y autenticación mediante esquemas de cifrado como AES CTR, AES CCM, entre otros, los cuales deben ser aplicados a fin de evitar ser víctimas de ataques cibernéticos, la incorporación de herramientas de seguridad en la transmisión incrementa el consumo energético sin embargo no es recomendable bajo ningún punto de vista levantar un sistema sin medidas de seguridad.

3.4. Carcasas y encapsulados de los nodos sensores

Una de las consideraciones adicionales a tomar en cuenta es las características de la carcasa del nodo sensor, la misma debe ser capaz de brindar la suficiente protección ante las variables climáticas a los elementos que constituyen el nodo sensor. Dentro de las investigaciones revisadas existen diversas soluciones a este problema, desde cajas contenedoras impresas en 3D, o cajas de alojamiento comerciales con índices de protección IP certificados.

La figura 15 muestra el diseño de caja impresa en 3D, en la misma se puede apreciar además el panel solar acoplado en la carcasa, a continuación, la figura 16 muestra un contenedor plástico con perforaciones las cuales permiten la correcta detección de parámetros en el interior de la caja. En la figura 17, se aprecia una carcasa utilizada para el caso de un nodo sensor ubicado en el suelo, esta carcasa posee una IP67.

Figura 15.

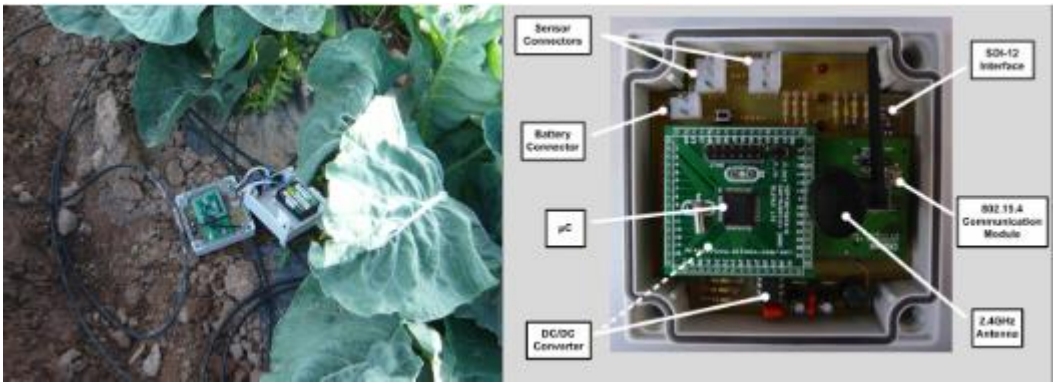
Ejemplo de carcasa impresa en 3D.

Figura 16.

Contenedor plástico para nodo sensor.

Figura 17.

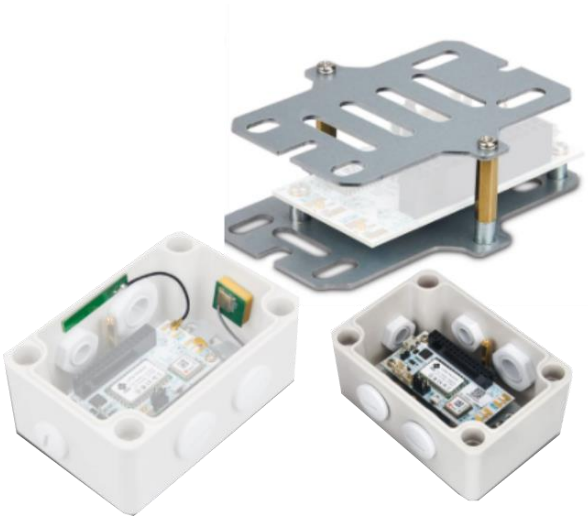
Carcasa de protección para nodo sensor ubicado al ras del suelo.



Adicionalmente se puede referir a diversos encapsulados comerciales existentes en el mercado, ver figura 18, los cuales buscan adaptarse a las necesidades de los desarrolladores e investigadores brindando diversas soluciones acordes a la necesidad. A continuación, se presenta como ejemplo un encapsulado con sus distintos accesorios que facilita la ubicación de elementos y componentes.

Figura 18.

Encapsulado comercial adaptable.



La tabla 9, muestra la descripción general de las carcasas utilizados en las arquitecturas desarrolladas.

Tabla 9.

Descripción de encapsulados y carcasas de protección de nodos sensores.

Trabajo	Contribución Técnica	Encapsulado / Protección
(Borrero & Zabalo , An autonomous wireless device for real-time monitoring of water needs, 2020)	An Autonomous Wireless Device for Real-Time Monitoring of Water Needs	Carcasa IP66
(Riquelme, y otros, 2009)	Wireless Sensor Networks for Precision Horticulture in Southern Spain	Watertight box IP67
(Visconti, de Fazio, Velasquez, Del Valle Soto, & Giannoccaro, 2020)	Development of Sensors-Based Agri- Food Traceability System Remotely Managed by a Software Platform for Optimized Farm Management	Caja de plástico con cubierta perforada
(Ilie-Ablachim, Pătru, Florea , & Rosner, , 2016)	Monitoring Device for Culture Sub- strate Growth Parameters for Precision Agriculture: Acronym: MoniSen	Impresión 3D ABS
(López , y otros, A multifunctional wireless device	GAIA2: A Multifunctional Wireless De- vice for Enhancing Crop Management	Carcasa impermeable diseñada para
(Valente, Silva, Duarte, Cabral Pinto, & Soares, 2020)	Low-Cost LoRaWAN Node for Agro Intelligence IoT	Carcasa impresa en 3D
(Estrada Mendoza, 2019)	Diseño de un nodo sensor para aplicaciones IoT	Carcasa IP67

Trabajo	Contribución Técnica	Encapsulado / Protección
(Pérez-Expósito, Fernández-Caramés, Fraga-Lamas, & Castedo , 2017)	An IoT Monitoring System for Precision Viticulture	Carcasa IP66
(Nurellari & Srivastava, 2018)	A Practical Implementation of an Agriculture Field Monitoring using Wireless Sensor Networks and IoT Enabled	Carcasa IP65

Existen diversos encapsulados para proteger las tarjetas controladoras y demás componentes electrónicos de los sistemas desarrollados, para la aplicación en la agricultura inteligente las cajas contenedoras tienen un papel importante puesto que las condiciones a los que están expuestas no son favorables. Se debe considerar que las especificaciones de las cajas contenedoras encajen perfectamente con el circuito implementado puesto cualquier modificación hace que pierda sus características e índices de protección.

3.5. Simulación como herramienta de análisis previo a la implementación

A continuación, se realiza el tercer experimento mediante el cual se expone algunas de las características de los nodos sensores que pueden ser analizadas a través de software de simulación, entre ellas está el consumo de energía, adyacencias y vecinos, número de saltos, análisis a través de exploradores web, establecimiento de routers de borde. Finalmente, se desarrolla un ejemplo de un servidor IoT en una red LAN, que puede ser implementado para la lectura de variables y datos tanto analógicos como binarios.

Existen varias plataformas sobre las cuales se pueden simular distintos escenarios, para el desarrollo de este apartado se utilizará el simulador contiki de cooja cuyas características fueron mencionadas en la sección anterior.

Contiki permite trabajar sobre una variedad de plantillas que se incluyen en su instalación, las cuales se pueden modificar de acuerdo a las características del proyecto, estas plantillas van desde sencillos ejemplos como el intercambio de saludos hasta códigos un poco más complejos como implementación de servidores MQQT, CoAP, RPL, manejo de protocolo UDP, dominios de broadcast, entre otros.

El primer ejemplo de simulación consiste en la edición de un script para modificar el mensaje de saludos entre nodos sensores y la verificación de intercambio de mensajes. La figura 19 muestra el código script que se ejecuta. En la figura 20 se observa los tipos de nodos sensores soportados por el software, así como la opción de importar nodos desarrollados en java que contemplen características particulares que pueden ser incorporadas.

Figura 19.

Script de intercambio de mensajes de saludo.

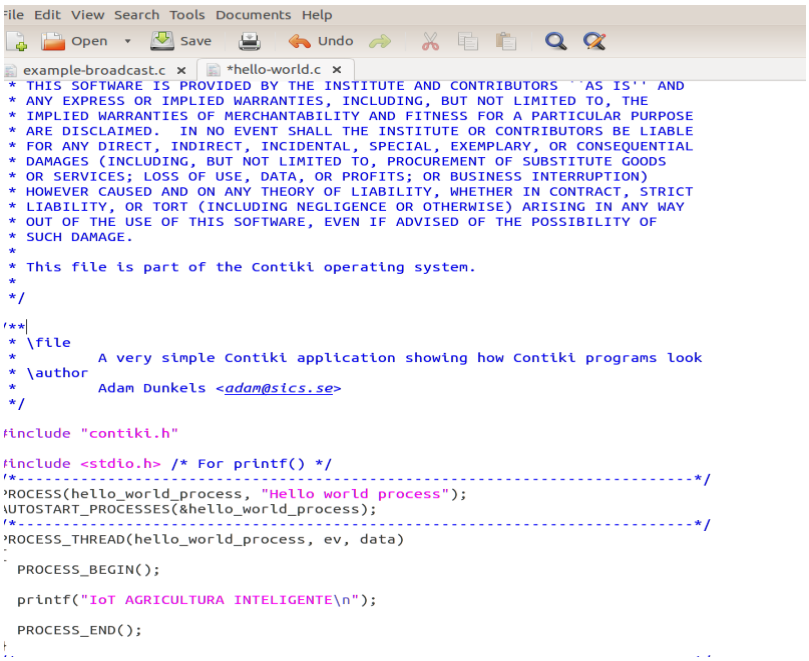
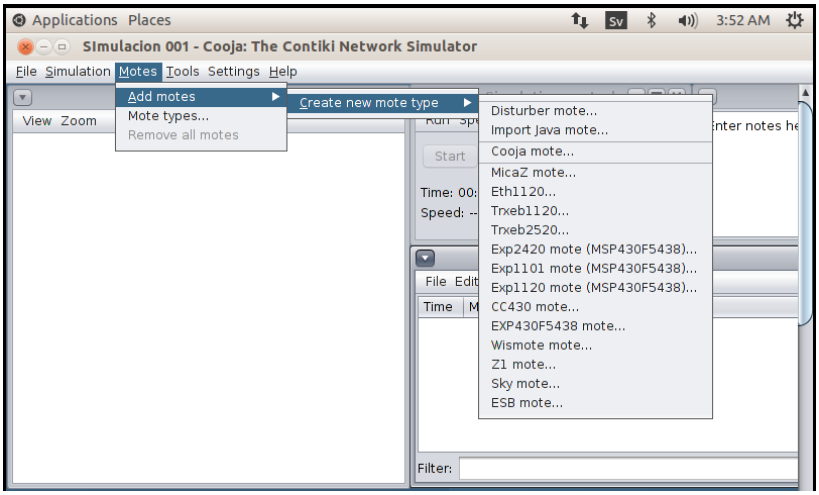


Figura 20.

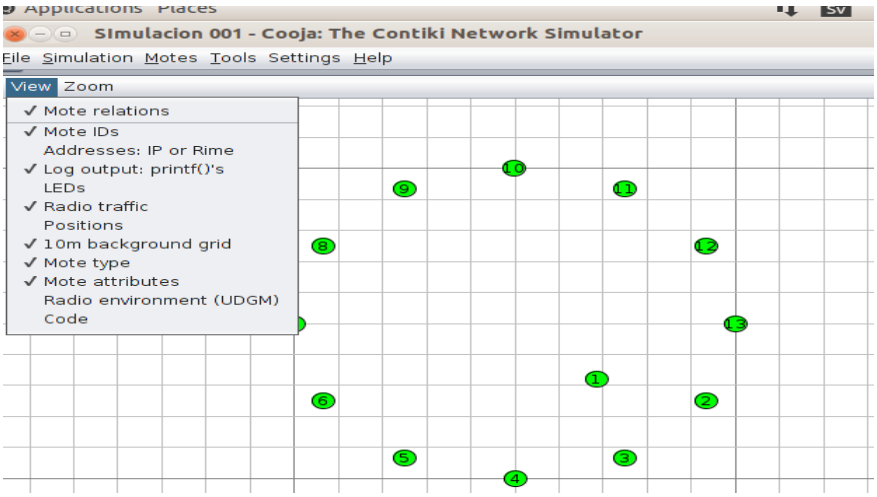
Nodos sensores disponibles para simulación



Una vez insertados los nodos sensores se puede establecer la distribución de los mismos en el plano XY, en la figura 21 se muestra una distribución y las propiedades de los nodos que se observa mientras se ejecuta la simulación como ID, trafico, posiciones, atributos, tipo entre otros. La figura 22 indica la ejecución de la simulación y el mensaje configurado para el ejemplo fue configurado “IoT Agricultura Inteligente”.

Figura 21.

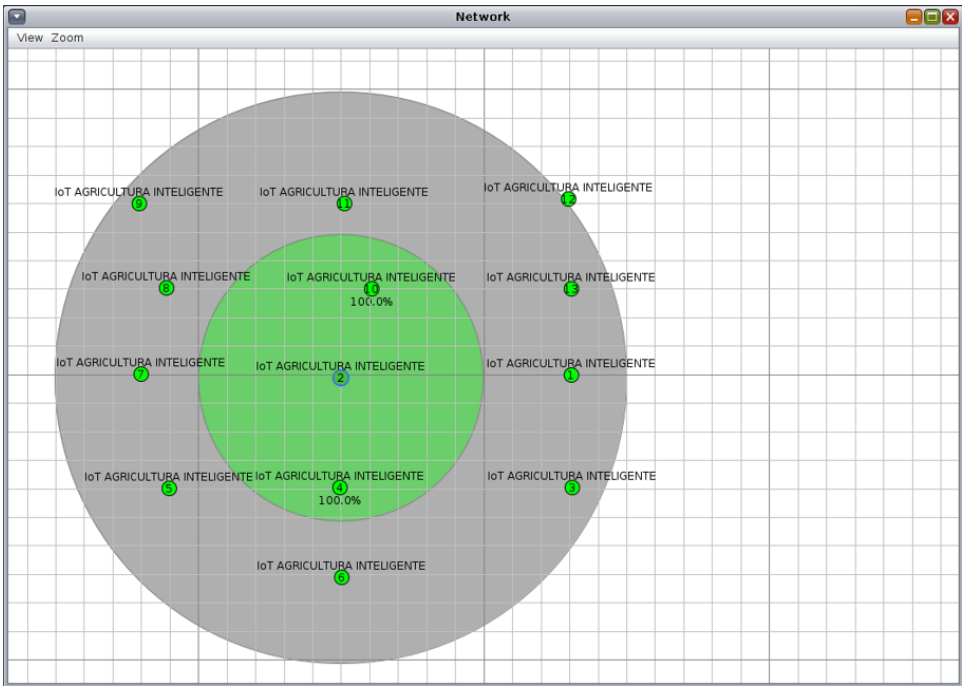
Nodos sensores y propiedades para análisis durante la simulación.



Nota. La ubicación de los nodos se expresa como una posición el plano XY, donde cada división representa 10m.

Figura 22.

Ejecución de la simulación, mensajes intercambiados.



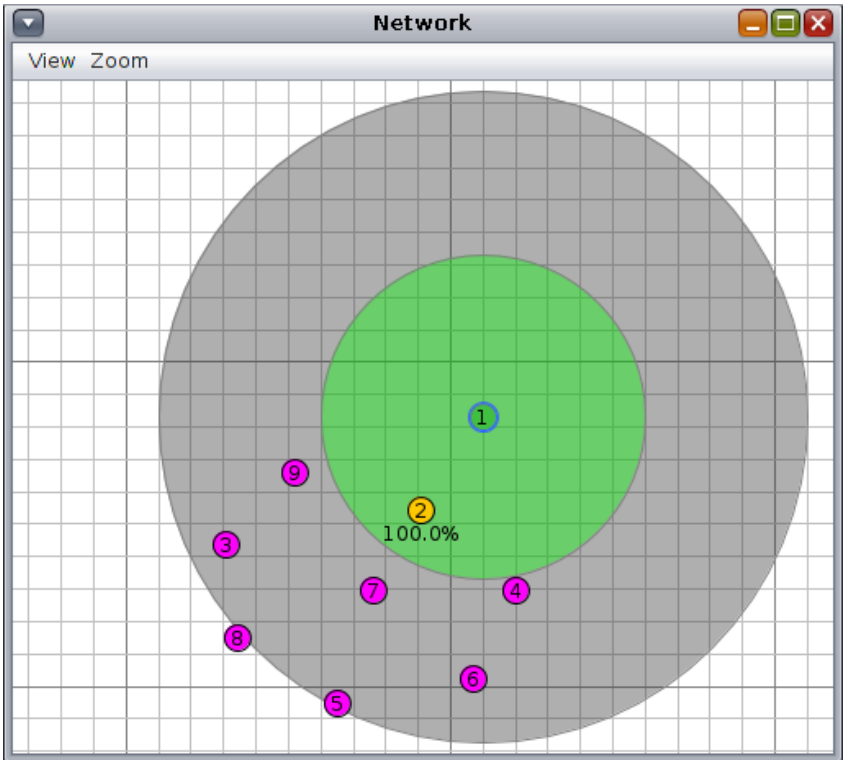
Nota. La ubicación de los nodos se expresa como una posición el plano XY, donde cada división representa 10m.

3.5.1. Simulación CoAP

A continuación, se realiza la simulación de CoAP en donde se evalúa el intercambio de mensajes y la convergencia de la red a través de la verificación del establecimiento de adyacencias. En la figura 23 se muestra la topología física para llevar a cabo esta simulación, en la cual se observa un total de nueve nodos sensores: un router de borde, un servidor y siete clientes.

Figura 23.

Topología física de los nodos sensores para simulación



Nota. La ubicación de los nodos se expresa como una posición el plano XY, donde cada división representa 10m.

Una vez establecida la disposición física de los nodos se procede a ejecutar el servidor correspondiente para el análisis de la red, para ello es necesario ingresar al directorio donde se encuentra el archivo de simulación y ejecutar el comando de ejecución del servidor, por ejemplo:

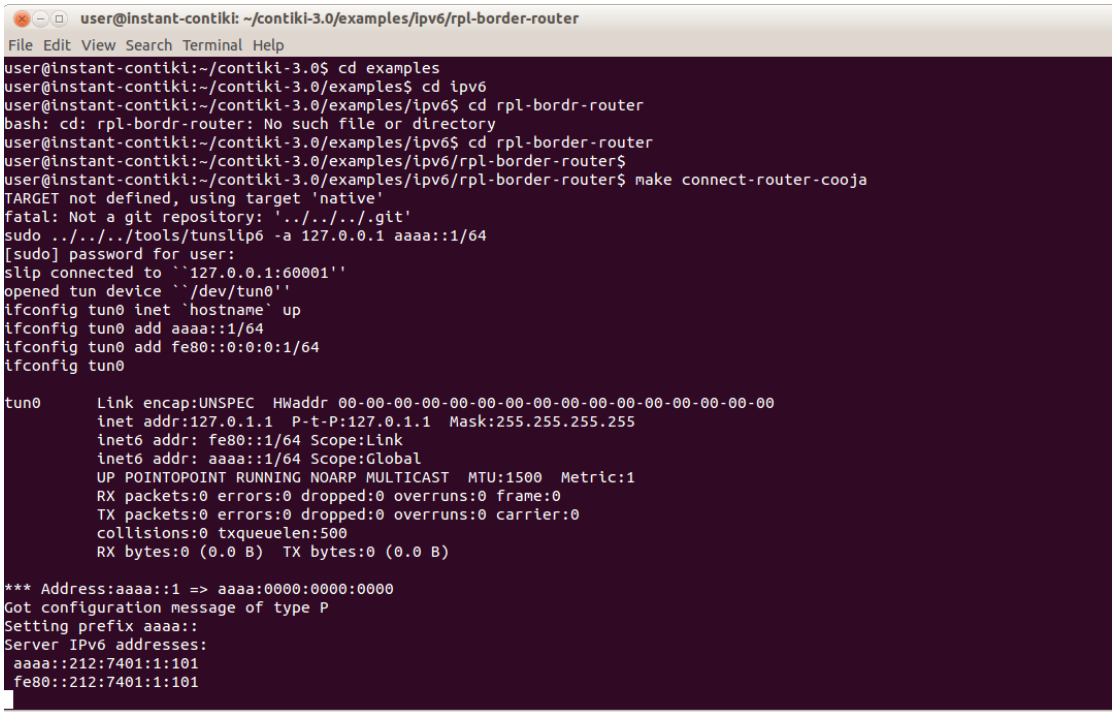
```
cd Contiki-3.0/ipv6/rpl-border-router

make_conect_router_cooja
```

Una vez ejecutado el comando, se tiene que verificar la dirección IPv6 asignada al servidor, en la parte inferior de la imagen 24, se puede verificar que la dirección en este caso es: aaaa::212:7401:1:101.

Figura 24.

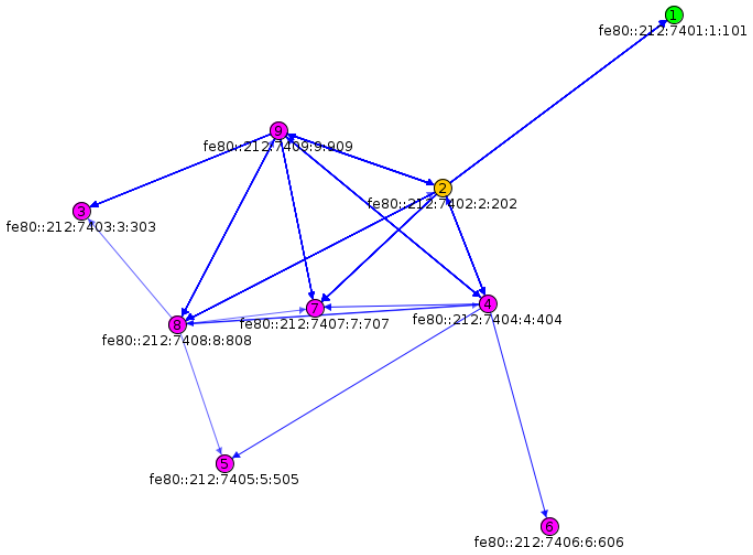
Ejecución del servidor y direcciones Ipv6.



A continuación, se inicia la simulación y observa el tráfico de datos generado por los nodos sensores como se aprecia en la figura 25. Además, se observa las direcciones Ipv6 de cada uno de los nodos

Figura 25.

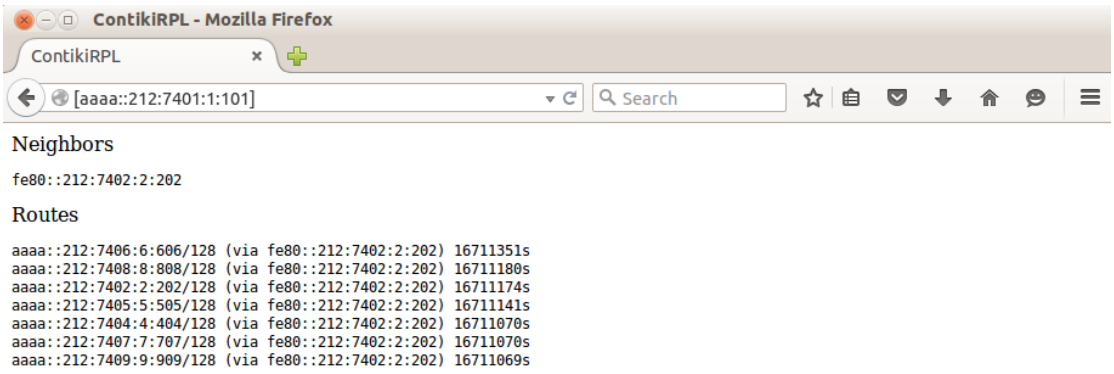
Tráfico de datos generado por los nodos sensores.



Para verificar el funcionamiento se puede acceder desde un navegador a la dirección del servidor y analizar el estado de la red, las rutas disponibles y las adyacencias o vecindades establecidas por el servidor, para el ejemplo la adyacencia del servidor es el nodo “2” o router de borde, además se puede verificar la convergencia de la red ya que se disponen de 7 rutas una por cada nodo cliente, ver figura 26.

Figura 26.

Verificación de rutas y adyacencias en el servidor.

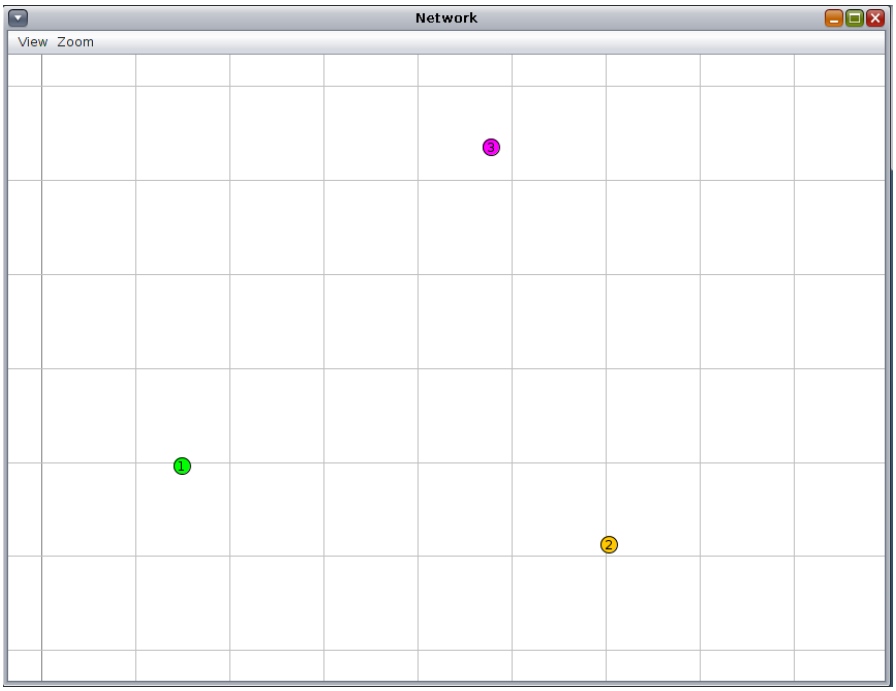


3.5.2. Simulación MQTT

Para efectuar la simulación de la ejecución del protocolo MQTT se establece un nodo suscriptor, un publicador y un bróker o servidor. Como se muestra en la figura 27.

Figura 27.

Escenario de simulación para protocolo MQTT.



Nota. La ubicación de los nodos se expresa como una posición el plano XY, donde cada división representa 10m.

El nodo 1 será el que actúe como broker por lo que se debe activar un servicio dentro del cual se tiene los tópicos de publicación y suscripción. Para ello es necesario ingresar al directorio de la carpeta que contenga los archivos del servidor y ejecutar el comando de inicialización del servidor.

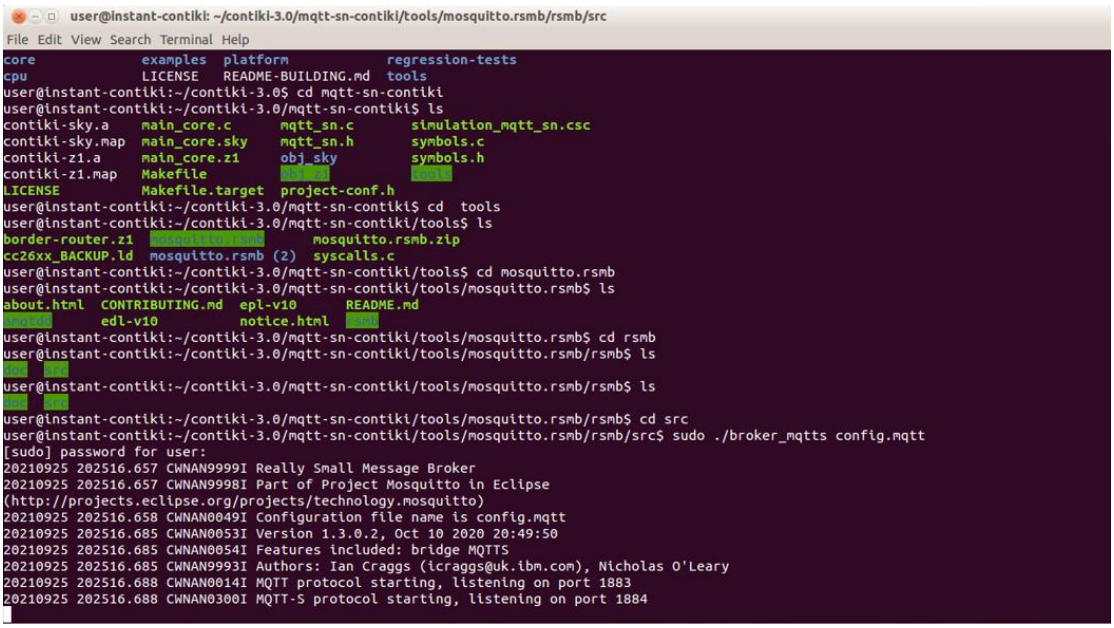
```
cd Contiki-3.0/mqtt-sn-contiki/tools/mosquito.rsmb/rsmb/src

sudo ./ broker_mqtts config.mqtt
```

Si la instrucción se ejecuta sin errores se deberá visualizar el mensaje de habilitación del puerto mediante el mensaje `listenig on port 1884`, similar a la figura 28.

Figura 28.

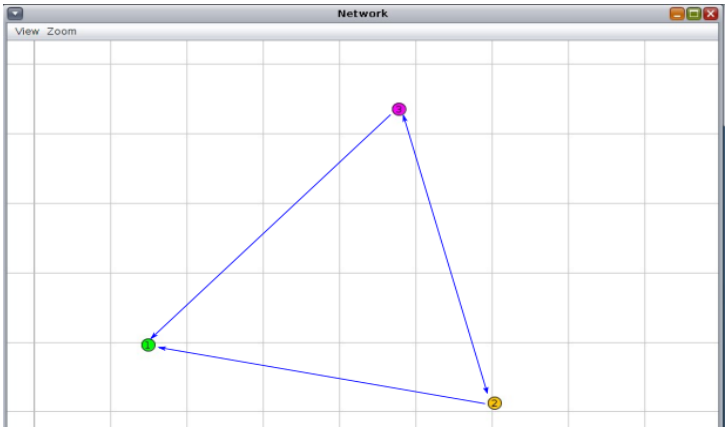
Ingreso al directorio e instalación del servidor MQTT.



Una vez que el servidor se encuentra ejecutándose y escuchando por los puertos asignados se procede a correr la simulación, la figura 29 muestra el tráfico de red generado entre los nodos sensores mientras que en la figura 30 se puede verificar los mensajes intercambiados, la inicialización del servidor y los demás nodos sensores.

Figura 29.

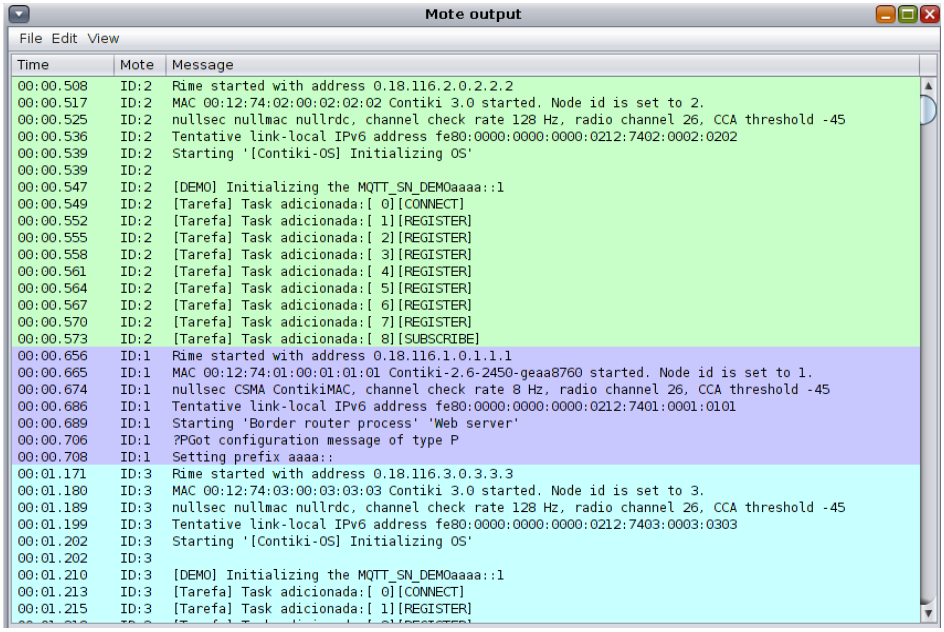
Tráfico de datos generados durante la simulación.



Nota. La ubicación de los nodos se expresa como una posición el plano XY, donde cada división representa 10m.

Figura 30.

Mensajes en la inicialización de la simulación.



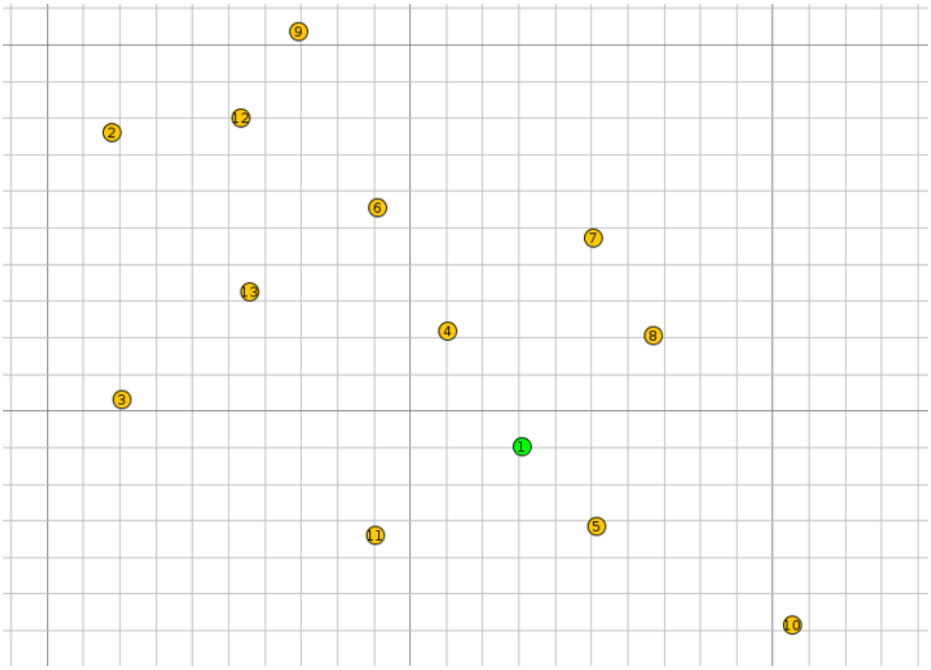
3.5.3. Monitoreo de Parámetros de la Red

Para analizar y evaluar diferentes situaciones se establece una topología física que contempla varias situaciones: retransmisión de paquetes hacia el servidor, verificación de adyacencias, convergencia de la red, consumo energético instantáneo y promedio, estas situaciones son analizadas más adelante y el escenario se indica en la figura 31, en la cual se tiene un nodo que hace las veces de router/servidor y puede manejar más de un protocolo y doce nodos sensores que recopilan y transmiten datos.

En la figura 32 se puede apreciar que varios nodos están por fuera del área de cobertura del nodo servidor, sin embargo, éstos pueden transmitir sus datos hasta el nodo 1, como se analiza más adelante existen rutas que implican retransmisión y por ende un incremento en el número de saltos.

Figura 31.

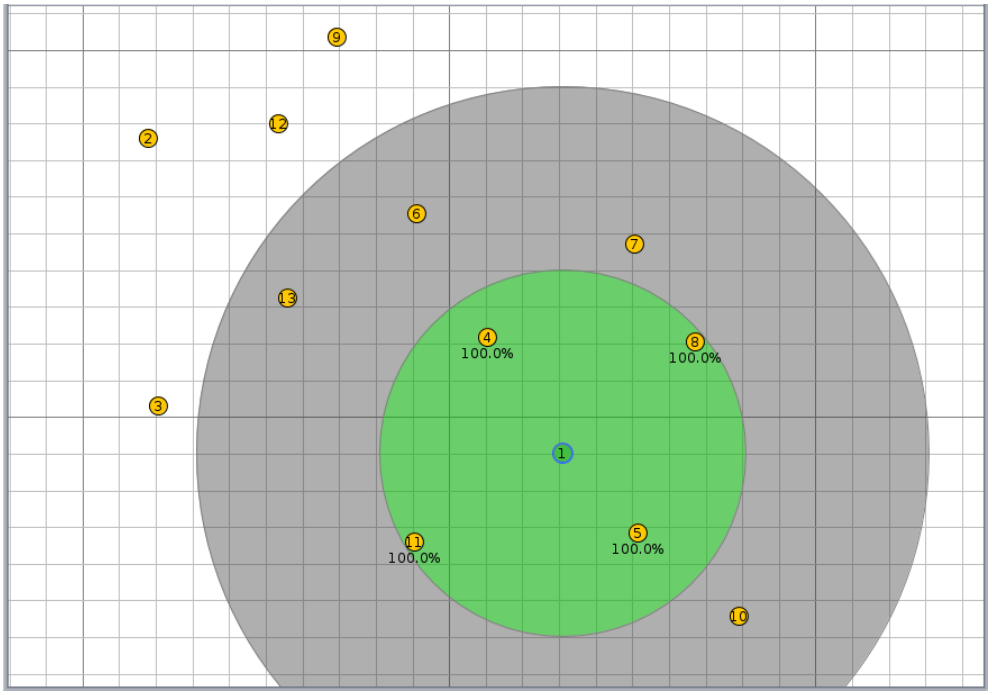
Topología física para el escenario de simulación de recopilación de datos.



Nota. La ubicación de los nodos se expresa como una posición el plano XY, donde cada división representa 10m.

Figura 32.

Radio de cobertura del nodo servidor.

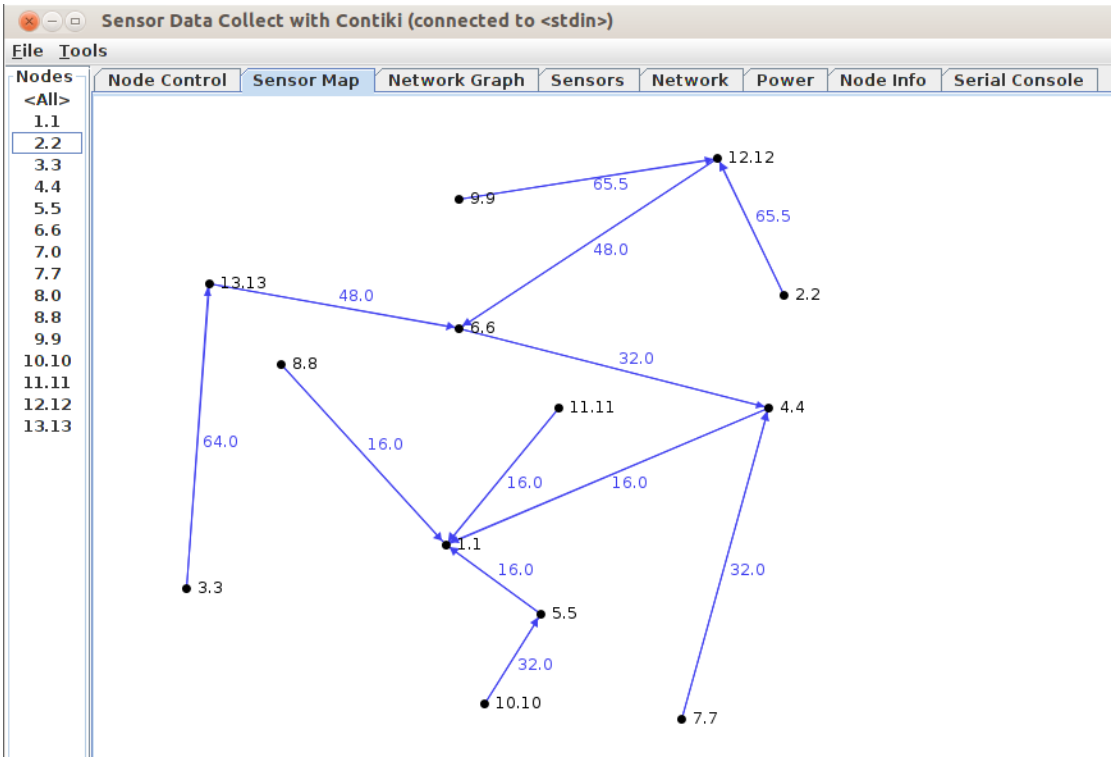


Nota. La ubicación de los nodos se expresa como una posición el plano XY, donde cada división representa 10m.

A continuación, en la figura 33 se puede observar la topología lógica de la red en función de la cual se verifica cómo los nodos sensores se comunican con el nodo 1.1 que es el servidor. En azul se muestran los costos establecidos para cada ruta, por ejemplo, los nodos 4.4, 5.5,8.8 y 11.11 son los nodos con acceso directo al nodo 1.1 y en consecuencia tienen un costo de 16. EL nodo 6.6 tiene un salto puesto que se comunica a través del nodo 4.4 y por lo tanto su costo es mayor. De esta manera se puede analizar la forma de acceso a la red de los nodos y definir las mejores posiciones a fin de establecer rutas redundantes y evitar puntos únicos de falla.

Figura 33.

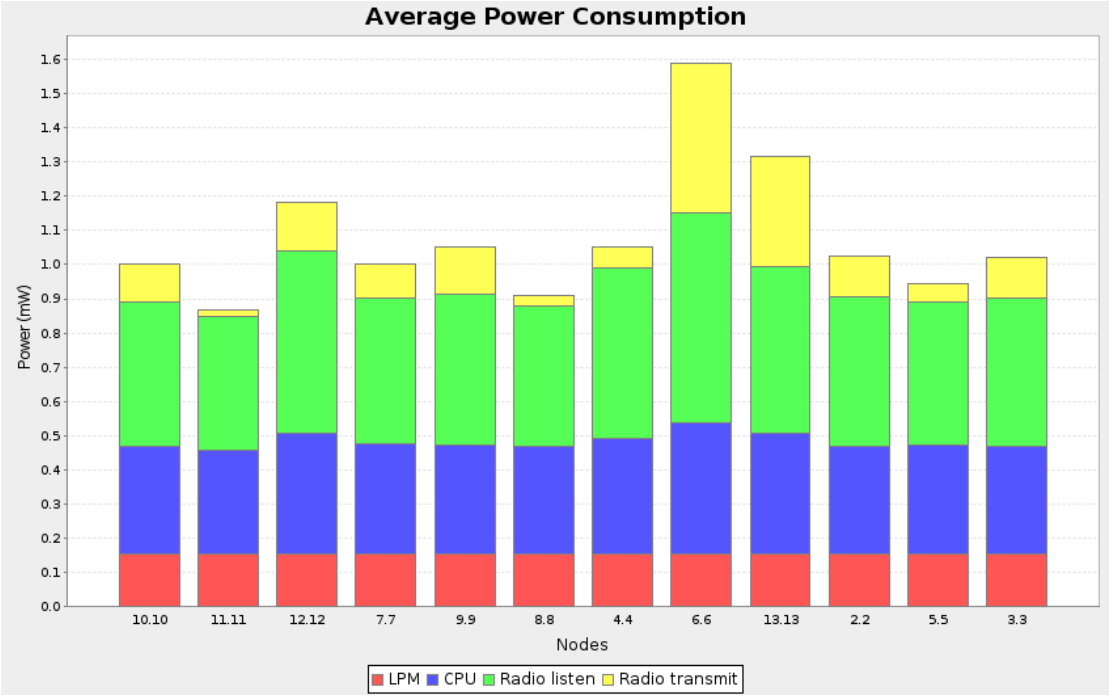
Topología lógica de la red.



Se debe tener presente que un nodo que retransmite paquetes de sus nodos adyacentes tendrá un mayor consumo energético, como se muestra en la figura 34, en la que se indica el consumo de energía promedio, el nodo 6.6 presenta un gasto energético mayor debido a que se convierte en la ruta de salida de los nodos 2.2, 12.12 y 9.9 hacia el nodo 1.1, mientras que el nodo 11.11 presenta el menor consumo puesto que es el único nodo que no realiza ninguna retransmisión ya q su única comunicación es con el servidor de manera directa, para este análisis se contempla los 3 modos de operación de los nodos sensores descritos anteriormente: transmisión/recepción (radio listen, radio transmit), modo procesamiento de datos (CPU) y el modo sleep (LPM o low power mode).

Figura 34.

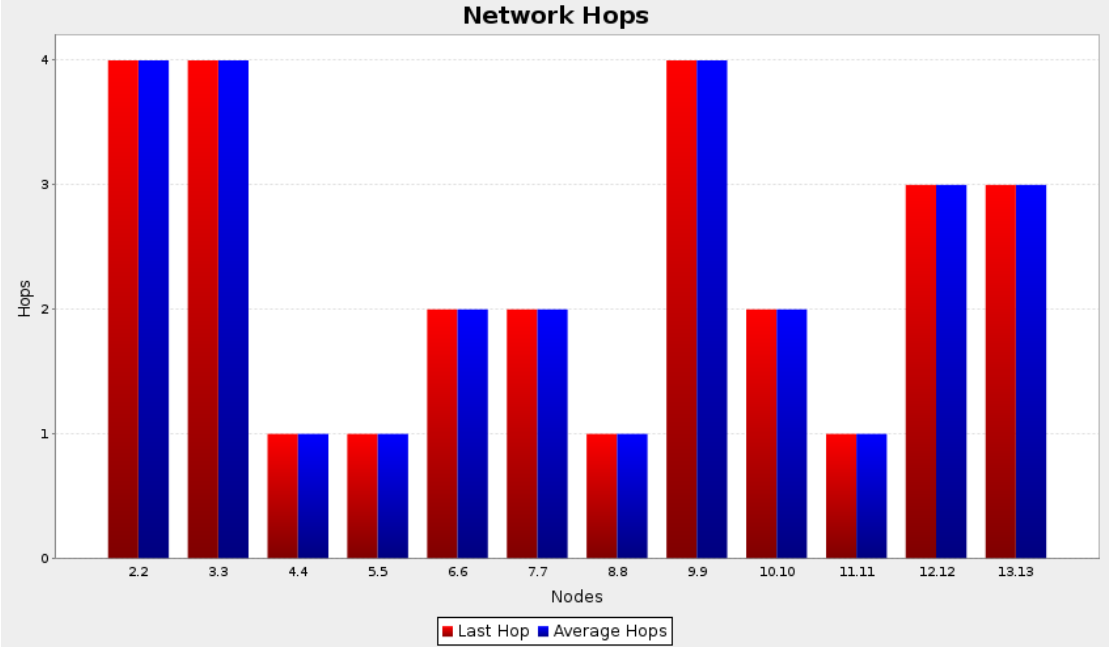
Gráfica de consumo promedio de energía por nodo.



Es importante conocer el número de saltos de cada nodo, a fin de establecer la ruta por la que se está llevando a cabo la comunicación de cada nodo, esta información se muestra en la figura 35. En la que se puede verificar que los nodos que están dentro del radio de comunicación directa con el servidor tienen un solo salto como es el caso de los nodos 4.5, 5.5,8.8 y 11.11, los nodos 6.6 y 7.7 están a 2 saltos, los nodos 12.12 y 13.13 tienen 3 saltos y finalmente los nodos 2.2, 3.3 y 9.9 tienen 4 saltos.

Figura 35.

Número de saltos por cada nodo.



A continuación, en las figuras 36 y 37 se presentan el análisis de la métrica de 2 nodos en los cuales se puede apreciar la variación de la misma hasta que se logra la convergencia de la red y luego se tiene una estabilidad permanente, con lo cual se podría determinar si en la red existen intermitencias como las que se muestran en la figura 38, en donde se ve un reinicio del cálculo de la métrica. El análisis general de la métrica de la red se lo puede hacer con el promedio de la misma y se muestra en la figura 39.

Finalmente, en las imágenes 40 y 41 se muestra el análisis de métrica y vecindades de todos los nodos, en las cuales se observa que la información que se dispone en el servidor corresponde a los 12 nodos del escenario de ejemplo, con lo que se comprobado la convergencia de la red. El análisis realizado de forma general se ha centrado en los parámetros de la red, debido a que los algoritmos de control implementados requieren un

análisis particular de la zona geográfica, condiciones ambientales y demás condiciones particulares del lugar donde se implementará el proyecto.

Figura 36.

Métrica promedio del nodo 6.6.

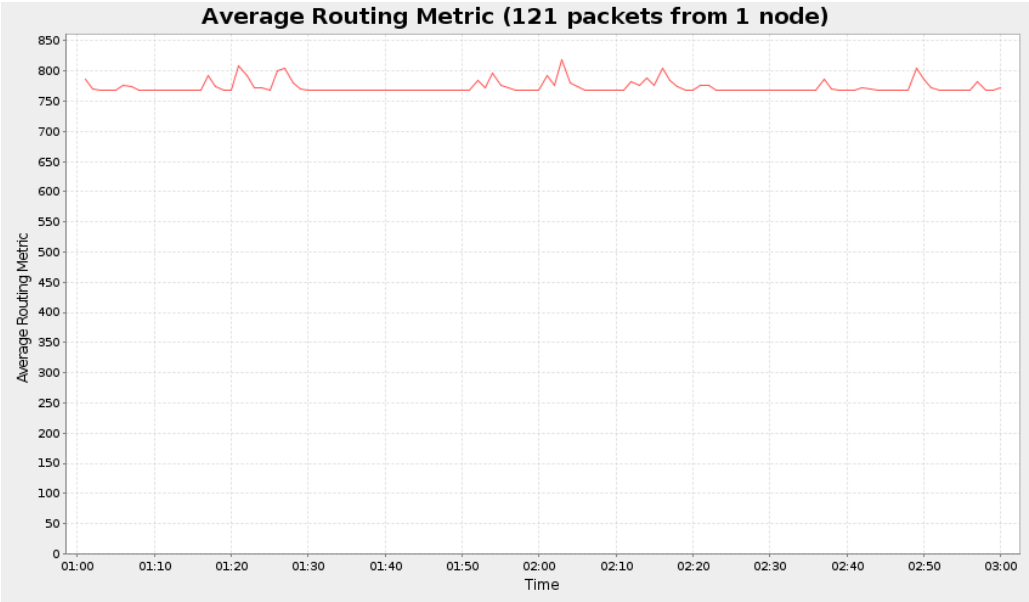


Figura 37.

Métrica promedio del nodo 10.10.

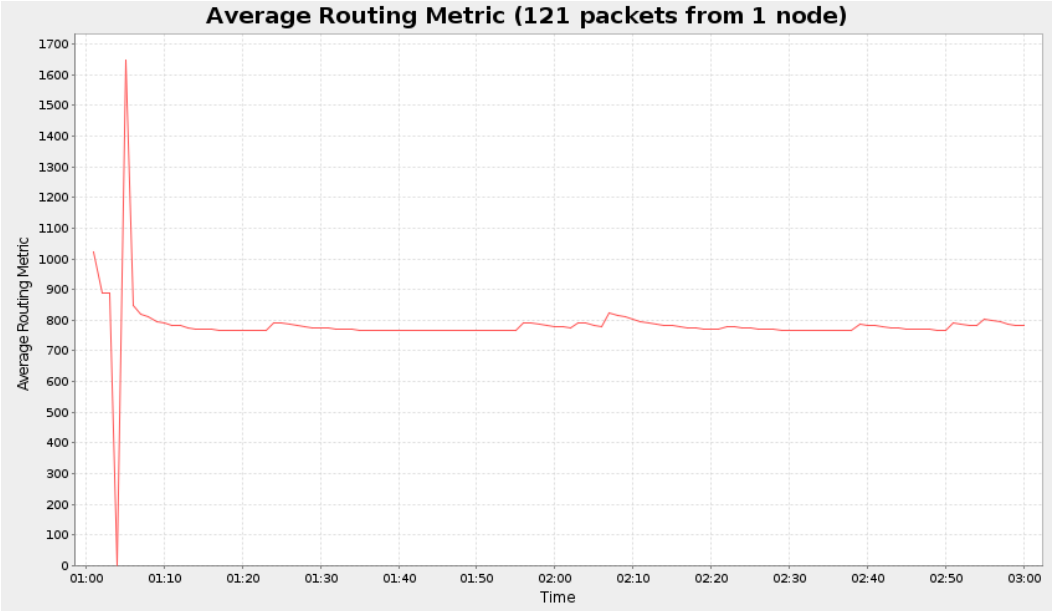


Figura 38.

Métrica del nodo 12, donde se observa un recálculo de la misma.

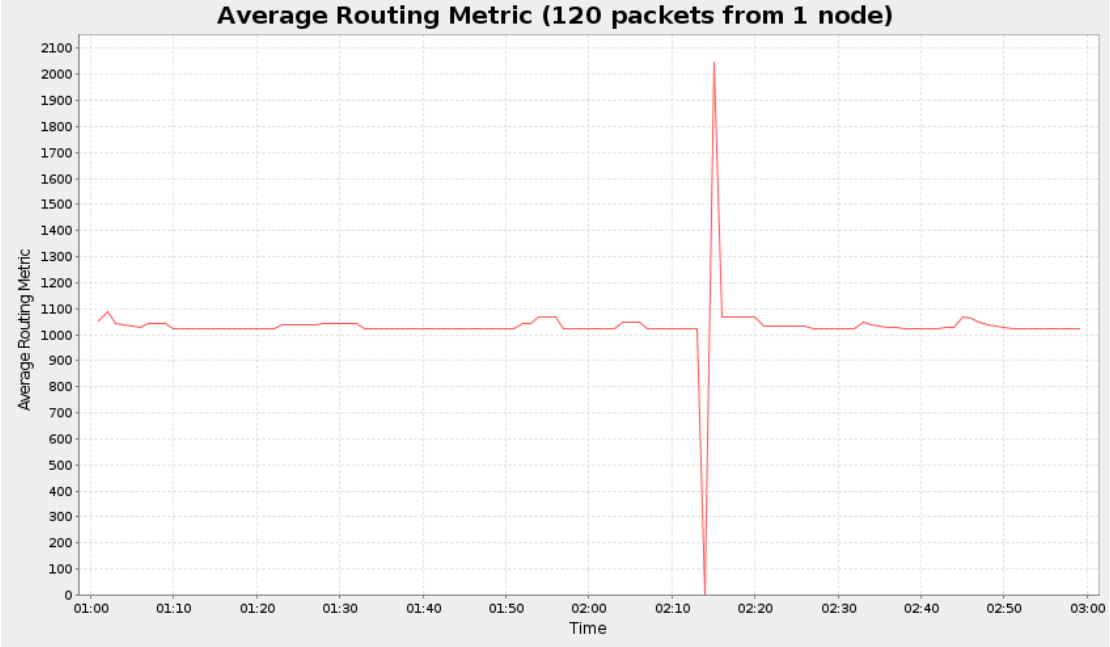


Figura 39.

Promedio de la métrica de todos los nodos sensores.

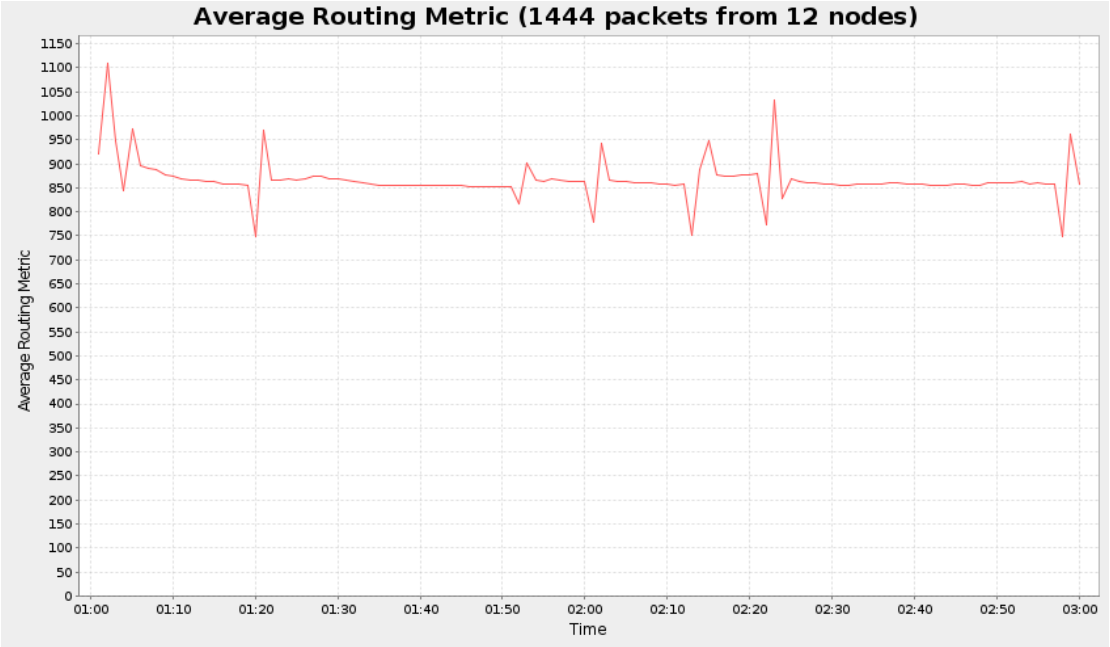


Figura 40.

Número de vecinos por cada nodo.

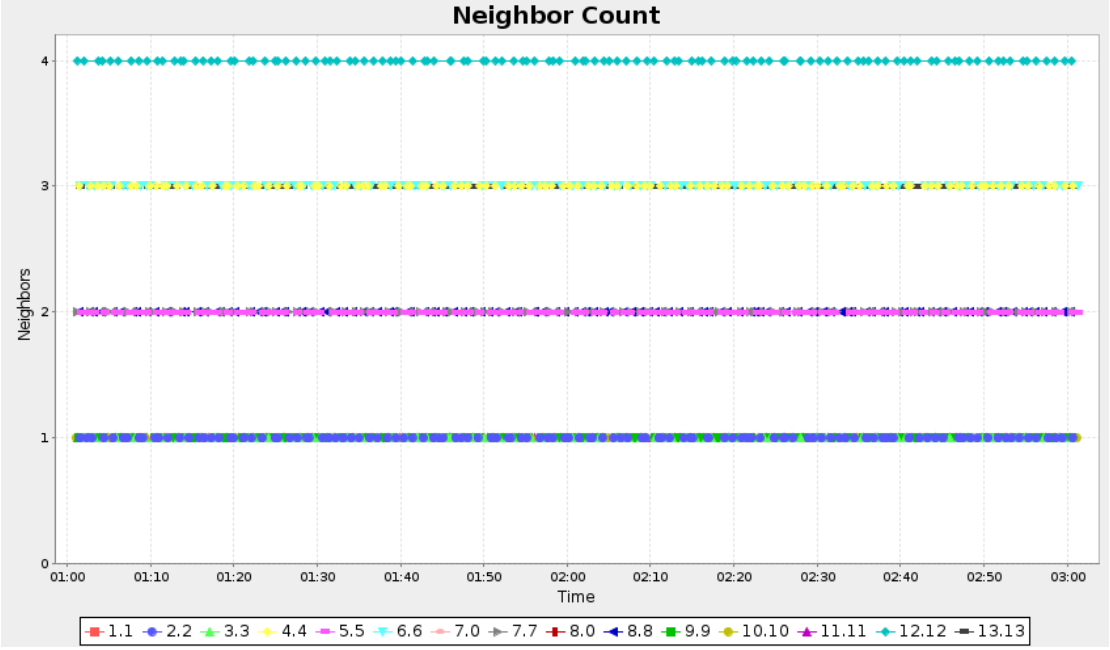
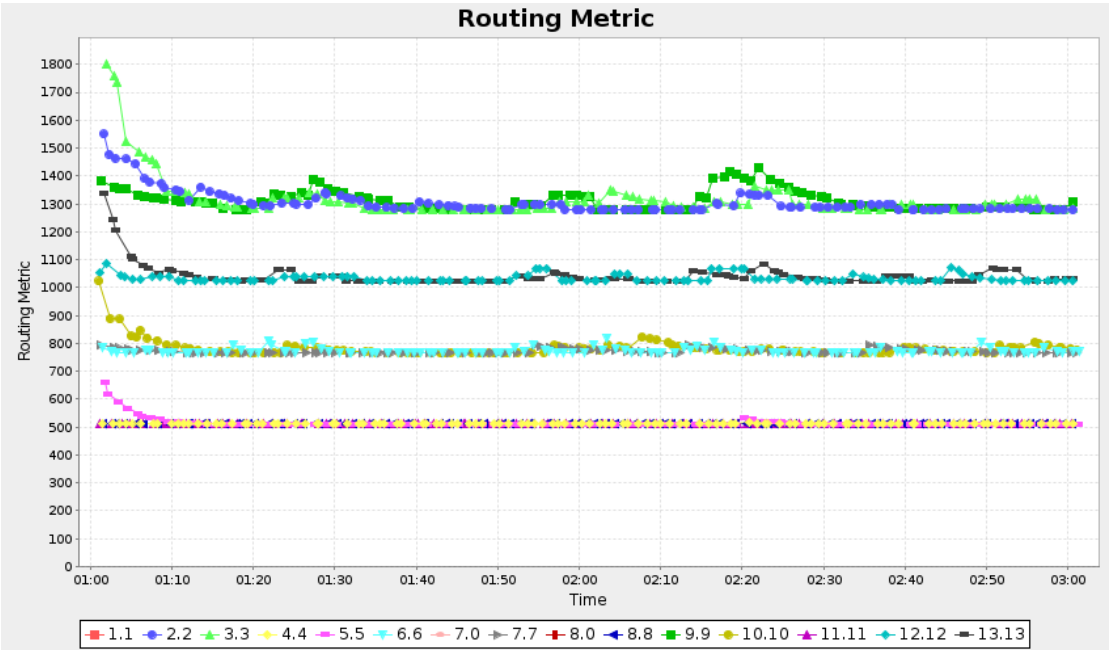


Figura 41.

Análisis de las métricas de cada nodo sensor.



Los parámetros que se puede analizar y dimensionar a través de simulación dan un aporte significativo para la consideración de ubicación de los nodos sensores, tiempos de transmisión, sistema de alimentación, a ser implementados en la arquitectura. Como se mencionó, las características particulares pueden ser incluidas al modificar los scripts de programación de los nodos sensores, incrementando la personalización y análisis particular en cada caso de estudio.

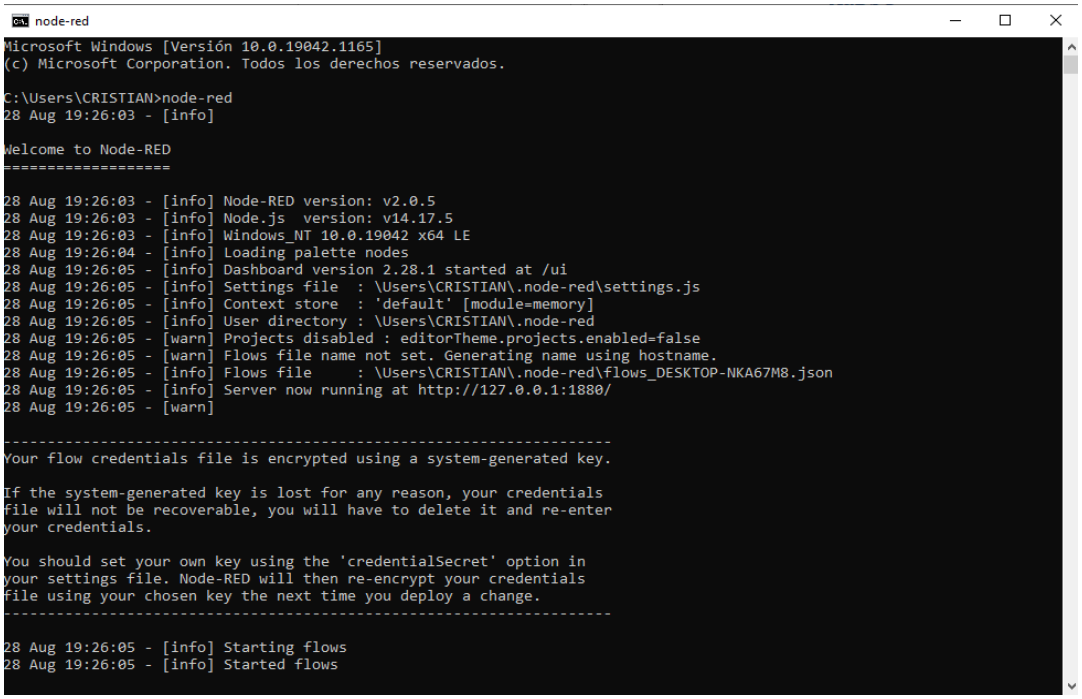
Finalmente se describe de forma general un servidor MQTT implementado en Node-Red y ejecutado en una red LAN, la ampliación de este servidor hacia el internet estaría sujeto al arrendamiento de una IP pública o el acceso a un servicio de hosting.

3.5.4. Ejemplo de implementación de un servidor MQTT

Para el ejemplo se ejecutará el servidor desde una PC con un sistema Operativo Windows 10, para ello es necesario instalar el software Nodejs. Posteriormente inicia la ejecución del servidor, para lo cual se de ejecutar el comando `node-red` y se mostrará una ventana similar a la mostrada en la figura 42, esta ventana no debe cerrarse mientras se desee que el servidor permanezca en ejecución.

Figura 42.

Ejecución de Node-Red



A la vez que se ejecuta Node-Red es necesario que se disponga de un servidor MQTT, para el ejemplo se aplica Mosquitto, para esto se debe ingresar el comando `mosquitto -v` en el directorio donde está instalado el servidor, como se muestra en la figura 43.

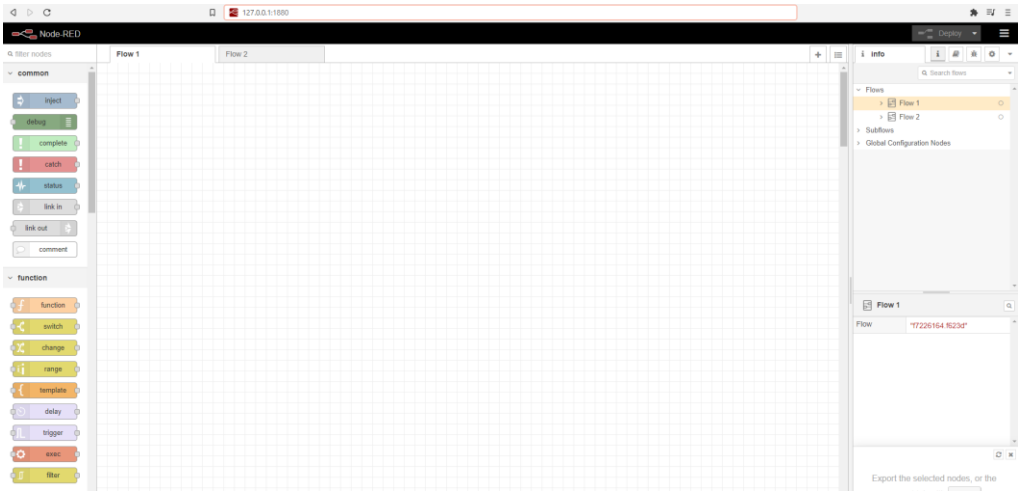
Figura 43.

Ejecución del servidor MQTT, Mosquitto.

Una vez que el servidor se encuentra en ejecución, desde cualquier navegador se ingresa a la dirección 127.0.0.1:1880, se accede a una pantalla como la que indica la figura 43, en la que se procede a realizar la programación del servidor MQTT, la creación de tópicos y pantalla de visualización.

Figura 44.

Ingreso a la interfaz de configuración Node-Red.



Para el desarrollo del ejemplo se considera la lectura y escritura de valores analógicos que permiten conocer el estado de una variable física o establecer un parámetro de SetPoint, y variables binarias mediante las cuales se ejecuta acciones on/off. La figura 45 muestra la pantalla de presentación del servidor en una computadora de la misma red LAN, mientras que en la figura 46 se observa el acceso a través de un dispositivo móvil.

Figura 45.

Ingreso a la interfaz del servidor desde una PC.

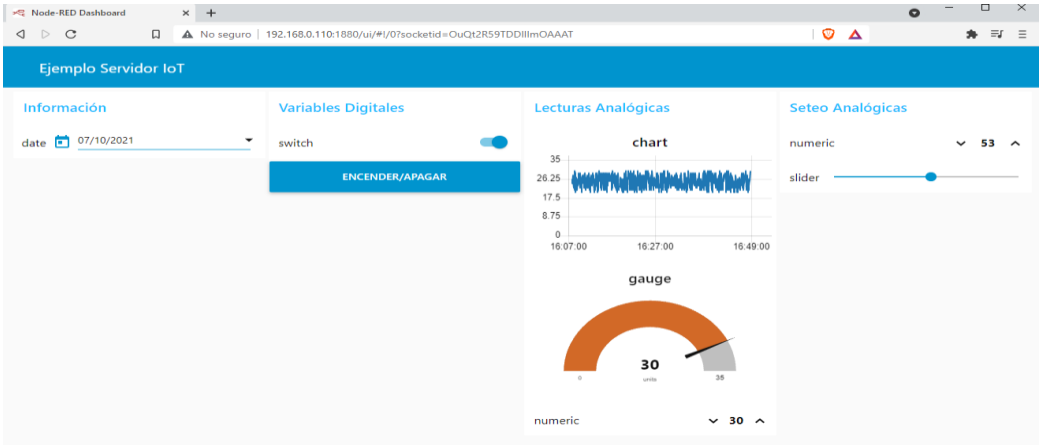
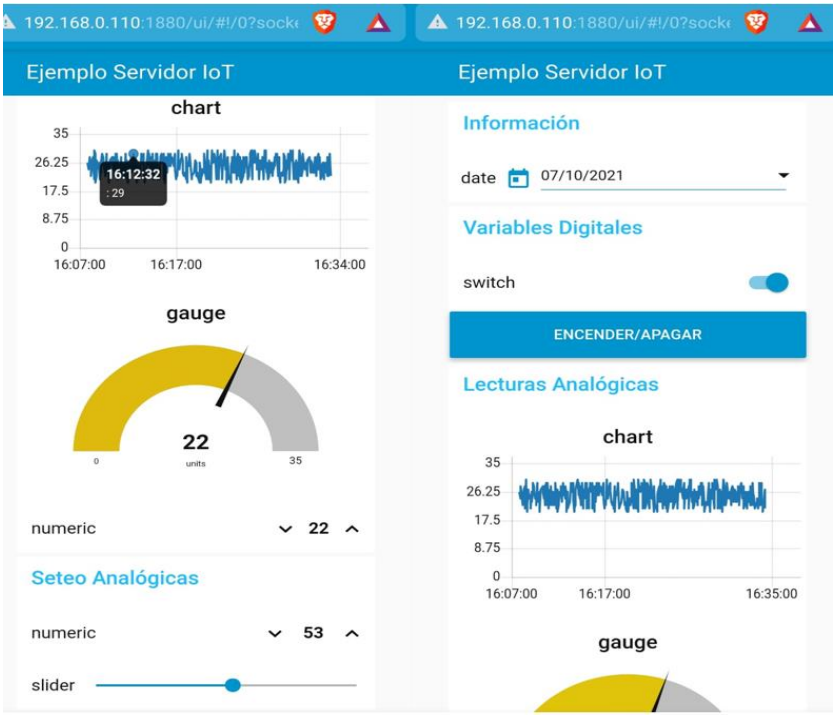


Figura 46.

Ingreso a la interfaz del servidor desde un dispositivo móvil.



La programación realizada se muestra en la imagen 47, en donde se verifica la conexión de los bloques de Node-Red con el servidor MQTT. Se puede verificar los datos recibidos si accedemos al servidor MQTT y al tópico específico mediante el comando:

mosquitto_sub -h [dirección IP] -t [tópico] o *mosquitto_sub -h localhost -t [tópico]*, como se indica en las figuras. Para la ejecución de este ejemplo se consideró únicamente 3 tópicos cuya recepción de información se verifica en las imágenes 48, 49 y 50, esta acción se la ejecuta desde el servidor, lo cual también puede considerarse como una herramienta de verificación en caso de errores en la comunicación en los tópicos creados.

Figura 47.

Programación desarrollada para la suscripción y publicación.

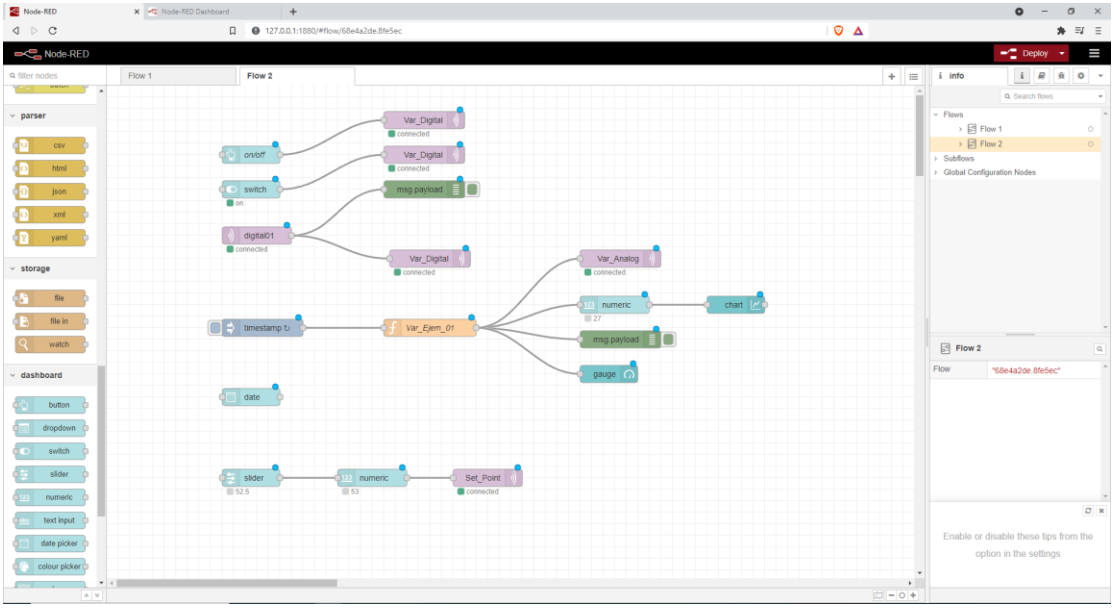


Figura 48.

Valores recibidos en el servidor MQTT, tópico Var_Digital.

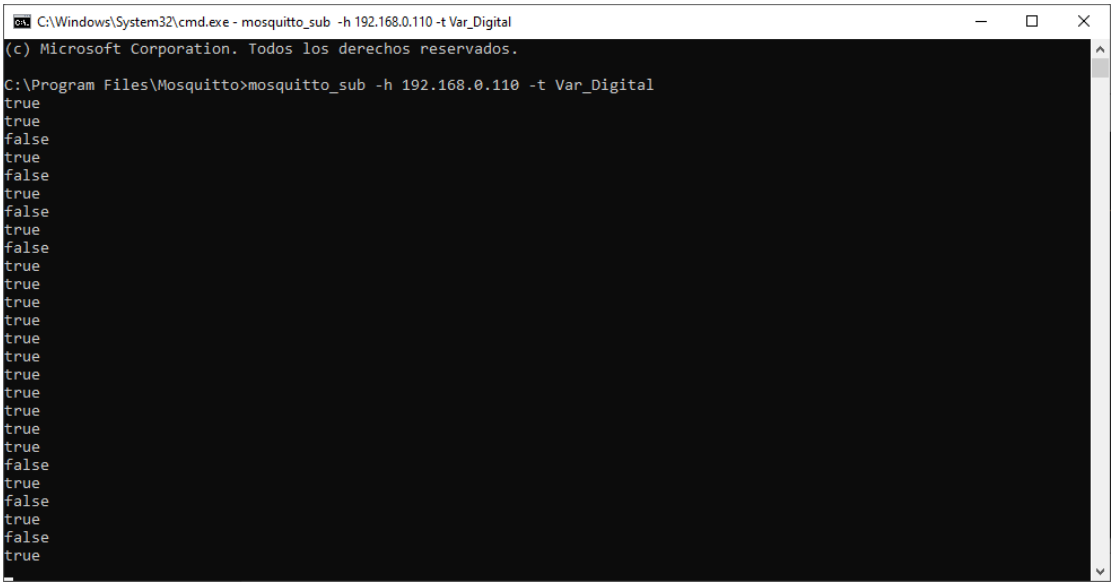


Figura 49.

Valores recibidos en el servidor MQTT, tópico Set_Point.

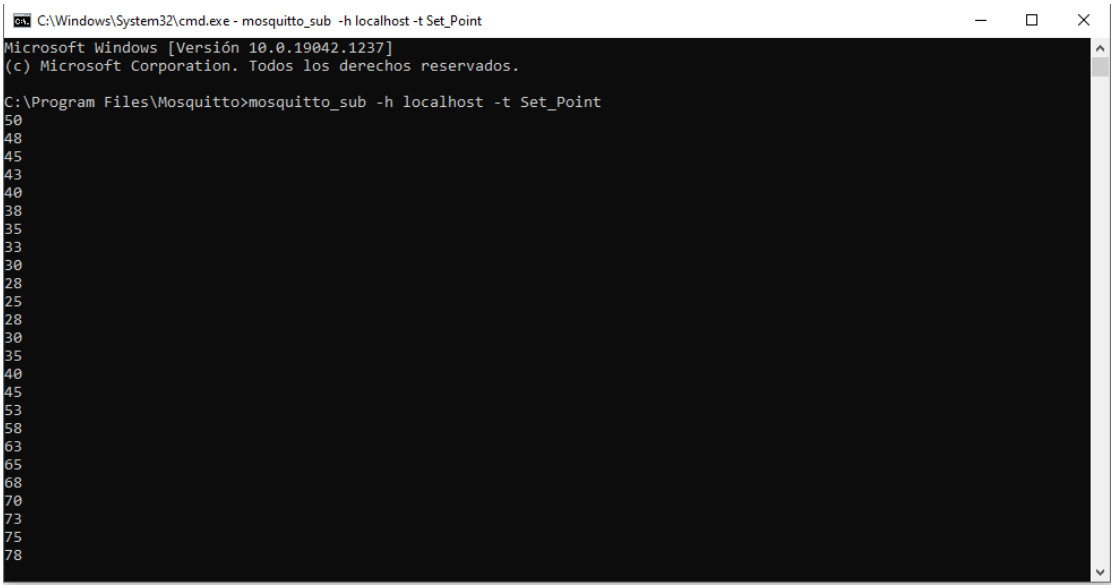


Figura 50.

Valores recibidos en el servidor MQTT, tópico Var_Analog.

En la última sección se ha evaluado el software de simulación como herramienta de análisis de proyectos de IoT en la agricultura inteligente, esta evaluación consiste en el análisis de parámetros de comunicación, convergencia de la red, transmisión de datos y consumo energético, exponiendo la potencialidad del software y su versatilidad para adaptarse a diferentes escenarios y requerimientos particulares.

3.6. Validación de la hipótesis

En los apartados que componen el presente documento se ha examinado diferentes conceptos, equipos y diversos componentes asociados a la inclusión del IoT en la agricultura inteligente, obteniendo conclusiones en base al análisis de diferentes artículos que describen trabajos desarrollados e implementados en este campo. A continuación, se describen algunos aspectos relevantes contenidos en los capítulos que anteceden:

Del primer experimento que consistió en el análisis bibliométrico se puede señalar que existe una estrecha relación entre la agricultura inteligente y los dispositivos aplicados en el IoT, marcando una tendencia de incremento en el número de trabajos publicados por año, además cabe señalar que los países que concentran el mayor número de investigaciones son India, China y Estados Unidos.

El segundo experimento consistió en el análisis documental, dentro del que se analizó la importancia y el tipo de encapsulados o carcasas que se han utilizado en diferentes aplicaciones y las prestaciones que éstos tienen en relación al ambiente en el que operan los nodos sensores. Dentro del estudio del consumo energético se hizo referencia a la generalización de los tres modos de operación que manejan tanto tarjetas de desarrollo, así como arquitecturas comerciales, para buscar la optimización del consumo energético y la extensión de su autonomía, se enfatizó a demás en la necesidad de la incorporación de sistemas de autocarga de baterías en los proyectos. Finalmente se efectuó un análisis de los ataques, así como de herramientas de mitigación cibernéticos que deben ser consideradas en la implementación de proyectos similares a fin de salvaguardar los datos e información generada.

En el tercer experimento se aplicó software de simulación en el cual se analizó parámetros de una arquitectura de IoT, detallando diferentes protocolos y elementos que pueden ser incorporados a los entornos simulados, demostrando de esta manera una versatilidad que puede considerarse para la evaluación de proyectos del IoT aplicado en la agricultura inteligente.

En base a la información contenida en el presente documento se puede afirmar que: el análisis de nodos sensores y protocolos de comunicación aplicados en la agricultura inteligente contribuye en el diseño y dimensionamiento de proyectos relacionados con la tecnificación agrícola, con lo que se valida la hipótesis planteada en el presente trabajo y se pone a disposición esta herramienta como referencia de partida para el desarrollo de otros proyectos dentro de éste ámbito.

Conclusiones:

- Se estableció 41 términos asociados con la cadena de búsqueda “IoT + Smart Agriculture”, agrupados en 4 clústeres, con un total de 762 enlaces entre sí, usando estos datos para definir las áreas de interés mediante el análisis documental, presentación, comparación y análisis de los datos.
- Las tarjetas de desarrollo, así como los nodos sensores comerciales presentan diferentes modos de operación con el objetivo de optimizar el consumo energético logrando autonomías especificadas desde los 14 hasta 724 días; la incorporación de sistemas alternativos de carga de baterías, generalmente mediante paneles solares, es una tendencia marcada en los proyectos desarrollados, con lo que se ha estimado tiempos de autonomía de hasta 1200 días.
- Los protocolos analizados tienen prestaciones de seguridad que incluyen encriptación y autenticación mediante esquemas de cifrado como AES-CTR, AES-CCM, entre otros, los cuales deben ser aplicados a fin de evitar ser víctimas de ataques cibernéticos, la incorporación de herramientas de seguridad en la transmisión incrementa el consumo energético sin embargo no es recomendable bajo ningún punto de vista implementar un sistema sin medidas de seguridad.
- Las cajas contenedoras utilizadas manejan índice de protección IP65 o superiores y juegan un papel importante puesto que las condiciones a los que están expuestas no son favorables. Se debe considerar que las especificaciones de las cajas contenedoras encajen perfectamente con el circuito implementado puesto cualquier modificación hace que pierda sus características e índices de protección, además de generar atenuaciones e interferencia a las antenas.
- Se aplicó el software Cooja de Contiki como una herramienta de análisis de proyectos de IoT en la agricultura inteligente, a partir de una topología compuesta por 13 nodos y un servidor realizó el análisis de parámetros de comunicación,

convergencia de la red, transmisión de datos y consumo energético, exponiendo la potencialidad del software y su versatilidad para adaptarse a diferentes escenarios y requerimientos particulares.

- Se implementó un servidor MQTT en Node-red para mostrar las funcionalidades disponibles en la lectura y escritura de datos para el control y monitoreo de variables físicas mediante la aplicación de IoT, diversas plantillas de servidores están disponibles en sitios de internet como GitHub las cuales se pueden modificar en función de las necesidades particulares de cada caso.
- Adicionalmente se elaboró el artículo “Sensor Nodes and Communication Protocols of the Internet of Things Applied to Intelligent Agriculture” que fue presentado en el 2nd International Conference on Applied Technologies ICAT2020 Latacunga, Ecuador. Anexo 1

Recomendaciones

- La implementación de una arquitectura IoT aplicada en la agricultura inteligente demanda el análisis de consumo energético puesto que la ubicación de los nodos sensores complica el acceso a una red eléctrica de suministro permanente. Por esta razón la mayor parte de trabajos analizados hacen énfasis en la integración de sistemas de auto carga de la batería mediante energías alternativas.
- Siempre se debe utilizar las herramientas de seguridad, encriptación, autenticaciones disponibles en cada protocolo a utilizar en la implementación de proyectos de IoT, para prevenir o mitigar un posible ataque cibernético.
- Es importante analizar los puntos críticos de comunicación y de ser necesario implementar equipos de comunicación redundantes en los nodos de borde ya que la caída o pérdida de comunicación con estos nodos traen consigo una pérdida de comunicación con toda la infraestructura desarrollada.
- Se recomienda establecer un plan de monitoreo de consumo energético de los nodos sensores porque una variación excesiva en uno o más nodos puede revelar un intento de violación a la seguridad de red implementada debido a que un nodo que es atacado presenta mayor tiempo en modo de transmisión/recepción.
- Como trabajos futuros se pueden diseñar diferentes soluciones de IoT enfocados en la agricultura inteligente que incorporen nodos sensores que se ajusten a las necesidades del entorno, además se puede sugerir la incorporación de sistemas experto que colaboren en la toma de decisiones basados en el aprendizaje automático. Por otro lado, la estimación de autonomía de los sistemas se puede abordar mediante un análisis de los sistemas alimentación redundantes a partir de la recolección de energía de variables ambientales.

Bibliografía

(s.f.).

Abbasi, M. H., Yaghmaee, & Rahnama, F. (2019). Internet of things in agriculture: a survey. *3rd International Conference on Internet of Things and Applications (IoT)*, 1-12.

ADF. (2017). *Our converters for your conections*. Recuperado el 15 de Julio de 2021, de http://www.adfweb.com/Home/products/Ethernet_MQTT.asp?frompg=nav28_1&loc_phy=9069556&dg-k2=soluciones%20%2Biot&k001=b&d=c&pos=&kxyW=

Aldahdouh, K. A., Darabkh, K. A., & Al-Sit, W. (2019). A Survey of 5G Emerging Wireless Technologies Featuring LoRaWAN, Sigfox, NB-IoT and LTE-M. *In 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, 561-566.

Amarillo, & M. (2014). Simulaciónde RedeSde SenSoReS inalámbRicoS: un modelo eneRgéticoa nivelde nodo-SenSoR bajolaS eSpecificacioneSieee 802.15.4tmy Zigbe.

ANSYS. (10 de 03 de 2021). *ANSYS*. Recuperado el 08 de Agosto de 2021, de Industrial Internet of Things Trends (IIoT): https://www.ansys.com/technology-trends/iiot

Azure. (2021). *Azure*. Recuperado el 12 de Octubre de 2020, de Que es el IoT: https://azure.microsoft.com/es-es/overview/internet-of-things-iot/what-is-the-internet-of-things/#overview

Bevywise. (10 de 3 de 2021). Recuperado el 05 de Agosto de 2021, de An Exhaustive IoT Simulator for IoT/MQTT Application Testing: https://www.bevywise.com/iot-simulator/

Bonomi, F., Milito, R., Zhu, J., & & Addepalli, S. (2012). Fog computing and its role in the internet of things. *In Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 13-16.

Borrero, J., & Zabalo , A. (2020). An autonomous wireless device for real-time monitoring of water needs. *Sensors*, 2078.

Borrero, J., & Zabalo, A. (2020). An autonomous wireless device for real-time monitoring of water needs. *Sensors*, 20(7).

Catelani, M., Ciani, L., Bartolini, A., Guidi, G., & Patrizi, G. (2020). Characterization of a low-cost and low-power environmental monitoring system. *IEEE International Instrumentation and Measurement Technology Conference*, 1-6.

Chen, M., Miao, Y., Hao, Y., & Hwang, K. (2017). Narrow band internet of things. *IEEE access*, 20557-20577.

Chiluisa, G., Lagla, J., Rivas, D., & Alvarez, M. (2021). Intelligent monitoring system of environmental biovariables in poultry farms. *Advances in Intelligent Systems and Computing,*, 386–399.

Cisco Networking Academy. (12 de 10 de 2021). *Redes empresariales, Seguridad y Automatización.* Recuperado el 16 de Agosto de 2021, de Estado Actual de la Ciberseguridad: https://contenthub.netacad.com/ensa-dl/3.1.1

Deepa, C. A. (2021). smart agriculture using iot. *Advances in Intelligent Systems and*, 11-19.

Dignani, J. (2012). Análisis del protocolo ZigBee. *PhD thesis, Universidad Nacional de la Plata*.

Envira. (2018). Recuperado el 15 de Julio de 2021, de https://enviraiot.es/sectores/smart-agro/

Escorcia Otalora, T. A. (2008). El análisis bibliométrico como herramienta para el seguimiento de publicaciones científicas; tesis y trabajos de grado. 15-16.

Estrada Mendoza, P. (2019). Diseño de un nodo sensor para aplicaciones iot.

Feng, X., Yan, F., & Liu, X. (2019). Study of wireless communication technologies on Internet of Things for precision agriculture. *Wireless Personal Communications*, 1785-1802.

Fraga Castro, A. (2015). Simulador cooja para wsn basado en el sistema operativo contiki. *Doctoral dissertation, Universidad Central" Marta Abreu" de Las Villas*.

García-Fallas, F. (2016). SESBeacon: Nodo sensor electrónico para alertas tempranas.

Gómez, R., Real, K., Morán, C., Grijalva, P., & Recalde, T. (2019). IoT Applications in Agriculture: A Systematic Literature Review. *2nd International Conference on ICTs in Agronomy and Environment*, 68-76.

Guardo, E., Di Stefano, A., La Corte, A., Sapienza, M., & Scatà, M. (2018). A fog computing-based iot framework for precision agriculture. *Journal of Internet Technology*, 1401-1411.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). A vision, architectural elements, and future directions. *Future generation computer systems*, 29.

Guerrero, F., Estrada-González, M., Medina-tejeda, M., Rivera-Gutierrez, J., & Alcaraz-Aguirre. (2017). Sgreenh-iot: Plataforma iot para agricultura de precisión. *Revista Iberoamericana de sistemas, cibernética e informática*.

Guerrero, J. A., Estrada, F. P., Medina, M. A., & Rivera, M. G. (2017). SgreenH-IoT: Plataforma IoT para agricultura de precisión. *Revista Iberoamericana de sistemas, cibernética e informática*.

Guillermo, C., García, A., Rivas, D., Huerta, M., & Clotet, R. (2018). IoT architecture based on wireless sensor network applied to agricultural monitoring: A case of study of cacao crops in ecuador. *International Conference of ICT for Adapting Agriculture to Climate Change*, 42-57.

Heble, S., Kumar, A., Prasad, K. V., Samirana, S., & Rajalakshmi, P. (2018). A Low Power IoT Network for Smart Agriculture. *EEE 4th World Forum on Internet of Things (WF-IoT)*, 609-614.

Heble, S., Kumar, A., Prasad, K., Samirana, S., Rajalakshmi, P., & Desai, U. (2018). A low power IoT network for smart agriculture. *IEEE 4th World Forum on Internet of Things (WF-IoT)*, 609-614.

Ilie-Ablachim, D., Pătru, G., Florea , M., & Rosner, , D. (2016). Monitoring device for culture substrate growth parameters for precision agriculture: Acronym: Monisen. *15th RoEduNet Conference: Networking in Education and Research*, 1-7.

Karim, .., Karim, F., & Frihida, A. (2017). onitoring system using web of things in precision agriculture. 402-409.

Khattab, A., Abdelgawad, A., & Yelmarthi, K. (2016). Design and implementation of a cloud-based iot scheme for. *28th International Conference on Microelectronics (ICM)*, 201-204.

Khattab, A., Abdelgawad, A., & Yelmarthi, K. (2016). Design and implementation of a cloud-based iot scheme for precision agriculture. 201–204.

Lain Holding. (2021). Recuperado el 25 de Julio de 2021, de https://lainholding.com/agricultura-de-precision-iot-sensores-inteligentes/

Libelium. (2020). Obtenido de https://www.libelium.com/iot-solutions/smart-agriculture/

Libelium. (2021). Recuperado el 22 de Junio de 2021, de https://www.libelium.com/

López , J., Navarro, H., Soto , F., Pavón , N., Suardíaz, J., & Torres, R. (2015). A multifunctional wireless device for enhancing crop management. *Agricultural Water Management*, 75-86.

López, J., Navarro, H., Soto, F., Pavón, N., Suardiaz, J., & Torres, R. (2015). GAIA2: A multifunctional wireless device for enhancing crop management. *Agricultural Water Management*, 75-86.

Lora Alliance. (2017). *Lora Wan security.* Recuperado el 15 de Agosto de 2021, de https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

Manivannan, T., & Radhakrishnan, P. (2020). A Comprehensive Analysis of Simulation Tools for Internet of Things. *Solid State Technology*, 461-471.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2017). Unlocking the Potential of the Internet of Things. *McKinsey Global Institute*.

Mathworks. (3 de 10 de 2021). *Mathworks*. Recuperado el 30 de Julio de 2021, de MATLAB y Simulink para aplicaciones IoT: https://la.mathworks.com/solutions/internet-of-things.html

Mekala, .. S., & P. Viswanathan. (2017). A survey: Smart agriculture iot with cloud computing,". *International conference on microelectronic devices, circuits and systems (ICMDCS)*, 1-7.

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (197-202). Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT. *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2018.

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2018). Overview of Cellular LPWAN Technologies for IoT Deployment:. *Second International Workshop on Mobile and Pervasive Internet of Things*, 197-202.

Monnit. (s.f.). Recuperado el 20 de Julio de 2021, de https://www.monnit.com/applications/agriculture-livestock-monitoring/

Muangprathub, J., Boonnam, N., Kajornkasirat, S., Lekbangpong, N., Wanichsombat, A., & Nillaor, P. (467-474). IoT and agriculture data analysis for smart farm. *Computers and electronics in agriculture*, 2019.

Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. *2017 IEEE international systems engineering symposium (ISSE)*, 1-7.

Nurellari, E., & Srivastava, S. (2018). A practical implementation of an agriculture field monitoring using wireless sensor networks and IoT enabled. *IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)*, 134-139.

Organización de las naciones unidas para la Alimentación y Agricultura. (12 de 09 de 2021). *Mecanización Agrícola Sostenible*. Recuperado el 10 de Julio de 2021, de Producción de cultivos: https://www.fao.org/sustainable-agricultural-mechanization/guidelinesoperations/cropproduction/es/

Patil, V. C., Al-Gaadi, K. A., Biradar, D. P., & Rangaswamy, M. (2012). Internet of things (Iot) and cloud computing for agriculture: An overview. *Proceedings of agro-informatics and precision agriculture (AIPA 2012)*, 292-296.

Pérez, M., Mendoza, M., & M., S. (2019). Paradigma IoT: desde su conceptualización hacia su aplicación en la agricultura.

Pérez-Expósito, T., Fernández-Caramés, T., Fraga-Lamas, P., & Castedo , L. (2017). An iot monitoring system for precision viticulture. *International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 662-669.

Priya, T., Praveen, K., & Srividya, A. (2013). Monitoring of pest insect traps using image sensors & dspic,". *Int. J. Eng. Trends Tech*, 4088–4093.

Rahman, T., & Chakraborty, S. K. (2018). Provisioning technical interoperability within Zigbee and BLE in IoT environment. *2nd International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, 1-4.

Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low power wide area networks: An overview. *ieee communications surveys & tutorials*, 855-873.

Riquelme, J., Soto, F., Suardíaz , J., Sánchez , P., Iborra, A., & Vera, J. (2009). Wireless sensor networks for precision horticulture in southern Spain. *Computers and electronics in agriculture*, 25-35.

Rueda, J. S., & Portocarrero, J. M. (2017). Similitudes y diferencias entre Redes de Sensores Inalámbricas e Internet de las Cosas: Hacia una postura clarificadora. *Revista Colombiana de Computación*, 58-74.

Sesé Vega, E. (2020). Estudio de las vulnerabilidades de la tecnología Bluetooth. *Estudio de las vulnerabilidades de la tecnología Bluetooth.*

Sichiqui, F., Huilca, J. G., García-Cedeño, A., Guillermo, J. C., Rivas, D., Clotet, R., & Huerta, M. (2019). Agricultural information management: A case study in corn crops in ecuador. *The International Conference on Advances in Emerging Trends and Technologies*, 113–124.

Singelée, D., & Preneel, B. (2006). Review of the bluetooth security architecture. In Information Security Bulletin.

Soni, D., & Makwana, A. (2017). A survey on mqtt: a protocol of internet of things (iot). *International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017*.

Stavrev, S. D., Terzieva, T. Z., & Golev, A. A. (2018). Integrating Third-party Services Using Brokers in the Serious Games Domain. *TEM Journal*, 842.

Tosi, J., Taffoni, F., Santacatterina, M., Sannino, R., & Fomica, D. (2017). Performance evaluation of bluetooth low energy: A systematic review. *Sensors*, 2898.

Valente, A., Silva, S., Duarte, D., Cabral Pinto, F., & Soares, S. (2020). ow-cost lorawan node for agro-intelligence IoT. *Electronics*, 987.

Verdouw, C. W. (2016). Internet of Things in agriculture. CAB Reviews: Perspectives in Agriculture, Veterinary Science, Nutrition and Natural Resources.

Visconti, P., de Fazio, R., Velasquez, R., Del Valle Soto, C., & Giannoccaro, N. (2020). Development of sensors-based agri-food traceability system remotely managed by a software platform for optimized farm management. *Sensors*, 3632.

VOSviewer. (23 de 10 de 2021). Recuperado el 19 de Agosto de 2021, de VOSviewer: https://www.vosviewer.com/

Yan, B., Yan, C., Ke, C., & Tan. (2016). Information sharing in supply chain of agricultural products based on. *Industrial Management and Data Systems*, 1397-1416.

Zhao, W., Lin, S., Han, J., Xu, R., & Hou, L. (2017). Design and implementation of smart irrigation system based on LoRa. *IEEE Globecom Workshops (GC Wkshps)*, 1-6.

Anexos