PANORAMA DE APLICACIÓN DE INTERNET DE LAS COSAS (IoT)

DAVID LEONARDO PINZÓN NIÑO

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2015

PANORAMA DE APLICACIÓN DE INTERNET DE LAS COSAS (IoT)

DAVID LEONARDO PINZÓN NIÑO

Trabajo presentado como monografía para obtener el título de Ingeniero de Telecomunicaciones.

Directora*:* Ing. Ángela Tatiana Zona Ortiz PhD.

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2015

TABLA DE CONTENIDO

TABLA DE IMÁGENES

TABLAS

1 INTRODUCCIÓN

El término de Internet de las Cosas (IoT) es importante para el desarrollo de los sistemas de tecnologías de la información y las comunicaciones, debido al planteamiento que muchos de los objetos o cosas que nos rodena estarán conectados por medio de Internet. Con el fin de integrar las cosas a esta red, es importante realizar una revisión de las tecnologías que permiten cumplir este propósito como son la identificación por radio frecuencia (RFID), los sistemas embebidos, la nanotecnología y redes de sensores.

Las tecnologías que soportan IoT, son muy amplias y su evolución constante. Debido a la revolución de internet que ha llevado a la interconexión entre las personas en una escala sin precedentes. Acelerando de esta manera la revolución que será la interconexión de los objetos para crear un entorno inteligente. Solo en el 2011, 9 millones de dispositivos se encontraban interconectados a nivel mundial, generando como expectativa la interconexión de 24 mil millones de dispositivos en el 2020 (Saint, 2015).

Esto se traduce en enormes cantidades de datos los cuales tienen que ser almacenados, procesados y presentados de una forma adecuada, eficiente y fácil de interpretar. Las prestaciones de IoT tanto para los usuarios como para la evolución de la tecnología serán siempre bajo demanda, garantizando una conectividad inteligente entre las redes existentes y calculando de manera adecuada los recursos sostenibles de la red (CÉSAR ANDRÉS GAVIRIA CUEVAS, 2014).

Sin embargo, la visión de IoT es ir más allá de los escenarios de computación móvil tradicional que utiliza los teléfonos inteligentes y portátiles, evolucionando en la

conectividad de objetos de la vida cotidiana mediante un ambiente tecnológico, con el objetivo de crear en los usuarios una adaptación a la nueva tendencia tecnológica.

Los dispositivos inteligentes, las arquitecturas de software y hardware, las redes de comunicación y todos los elementos necesarios para poder adoptar IoT, son parámetros relevantes a evaluar, ya que su finalidad es recolectar el mayor número de datos sin la intervención humana, de esta manera que se pueda brindar y proporcionar la mayor cantidad de información, para ser procesada y ayudar en la automatización del entorno (Jayavardhana Gubbi a, 2013). Por lo cual, se concluye que es importante realizar un panorama de IoT que permita generar futuras investigaciones al grupo de investigación INVTEL de la Universidad Santo Tomás.

2 PRESENTACIÓN DEL PROYECTO

2.1 PLANTEAMIENTO DEL PROBLEMA

La visión de IoT es utilizar tecnologías inteligentes para conectar objetos en cualquier lugar a cualquier hora. El internet de las cosas se ha convertido en una tendencia emergente para los investigadores en la academia y la industria, debido a las múltiples posibilidades de desarrollo que este genera. Cualquier marco para el desarrollo de aplicaciones para IoT debe ser compatibles, con los dispositivos y las nuevas tecnologías en desarrollo o despliegue, debido a que la idea fundamental de IoT es interconectar diferentes dispositivos (Objetos).

IoT hace que objetos reconocibles, puedan tener cierta inteligencia para comunicar información sobre ellos mismos o acceder a información que ha sido generada por otros objetos. El internet de las cosas proporciona una interacción entre los mundos real-físico y digital-virtual, a través de decisiones inteligentes haciendo uso de algoritmos en aplicaciones de software que permiten respuestas en un tiempo corto con el objetivo de poder recopilar información que sea usada en pro de la aplicación (Aditya Gaura, 2015).

Esto conlleva a una nueva dimensión de conceptos en los ámbitos de gestión de la cadena de suministros, transporte, logística, hogar, deporte, industria, energía, agricultura, comercio y educación. Siendo, de esta manera estos ámbitos un factor decisivo para el continuo desarrollo de IoT, ya que brinda la posibilidad de investigación mediante la oportunidad de crear y mejorar las tecnologías existentes.

La línea de investigación de interconexión y convergencia del grupo de investigación de la Facultad de Ingeniería de Telecomunicaciones INVTEL, incorpora la temática de IoT. Por lo tanto es necesario establecer el estado actual de esta tendencia con el objetivo de proponer iniciativas de investigación y aplicación, de modo que, la pregunta de investigación que se plantea es:

¿Cuál es el estado actual de desarrollo y aplicación de IoT y que oportunidades presenta para el grupo de investigación INVTEL?

2.2 JUSTIFICACIÓN Y PROPOSITO DE LA INVESTIGACIÓN

La función misional de investigación de la facultad de ingeniería de telecomunicaciones en coherencia con las instancias institucionales, define su misión como: Generar y apropiar conocimiento con sentido crítico e innovador desde un enfoque humanista a través de la I+D+I y la contemplación del entorno. Fortaleciendo la investigación, el talento humano y la gestión, con el fin de impulsar el desarrollo socio-económico sustentable del país transformándolo mediante el desarrollo y aplicación de las TIC (comité de investigación del 2 de julio de 2015).

El grupo INVTEL es el encargado de canalizar las iniciativas de investigación de la facultad, en el marco de la misión descrita anteriormente. El grupo INVTEL se creó en 2003, actualmente está reconocido por Colciencias y tiene categoría C, cuenta con 7 productos de nuevo conocimiento, 6 de desarrollo tecnológico, 15 de apropiación social del conocimiento y 11 de formación de recurso humano.

En el comité de investigación de la facultad de Ingeniería de Telecomunicaciones del 29 de abril de 2015, las líneas de investigación de INVTEL se ha redefinido como:

1. Regulación en TIC: Estudio tanto de la regulación como de la política relacionada en telecomunicaciones. Contemplando los requerimientos técnicos y normativos, implementación y seguimiento, y efectos en Colombia dentro de un marco global. Se incluye también la gestión del espectro.

2. Sistemas de Telecomunicaciones Definidos por Software: Estudio de los sistemas de comunicaciones, su desarrollo e implementación mediante software.
3. Dispositivos Radiofrecuencia, microondas y ondas milimétricas: Estudio de las técnicas de diseño y simulación de los dispositivos de un sistema de comunicaciones, en las bandas de radio, microondas y ondas milimétricas.
4. Gestión de las TIC en las organizaciones: Estudio de las mejores prácticas para la implementación y gestión de las TIC dentro de las organizaciones. Teniendo en cuentas los casos de aplicación de estándares, recomendaciones y metodologías relacionadas. Incluyendo la gestión de proyectos de telecomunicaciones.
5. Interconexión y convergencia: Estudio de interconexión y convergencia de servicios, contenidos, redes e infraestructura. Al igual que los factores y tecnologías que intervienen en el cambio tecnológico para el intercambio de información. Contemplando los temas relacionados con Internet de las cosas.

Como puede verse la línea de interconexión y convergencia incluye incursionar en la temática de IoT. Resultado de este interés la universidad participa en la creación de un Centro de Excelencia y Apropiación de Internet de las Cosas (CEA IoT) con el apoyo de Colciencias. Esta propuesta se presenta en el marco de una alianza entre la universidad Santo Tomás con la Pontificia Universidad Javeriana, HP y otras instituciones académicas y productivas.

Este es la razón fundamental para que desde el grupo INVTEL se genere un panorama actual de aplicación de IoT a nivel mundial. Este panorama permitirá establecer el cuerpo de conocimiento existente e identificar oportunidades de investigación.

2.3 OBJETIVO GENERAL

Establecer el cuerpo del conocimiento existente alrededor de la temática del internet de las cosas (IoT), mediante una revisión bibliográfica que permita identificar las oportunidades de investigación y desarrollo para fortalecer las iniciativas del grupo INVTEL.

2.3.1 OBJETIVOS ESPECIFICOS

- Establecer y clasificar el conocimiento especializado que circula en la sociedad relacionado con Internet de las Cosas (IoT).
- Establecer el estado de al menos 3 áreas de investigación y desarrollo para el despliegue de IoT.
- Establecer campos de aplicación de IoT que puedan generar iniciativas de investigación en IoT dentro del grupo de investigación INVTEL de la facultad de ingeniería de telecomunicaciones.

3 ANTECEDENTES PARA EL DESARROLLO DEL CONCEPTO IOT

En el año 2005 en la ITU (Unión Internacional de Telecomunicaciones) se nombra por primera vez el término de Internet de las Cosas (IoT por sus siglas en inglés, Internet of Things). Entonces se definió como la conexión en tiempo real de los objetos interconectados en una red permitiendo ser consultados por cualquier otro objeto que se encuentre en esta misma red.

Kevin Aston creador del internet de las cosas dice "es la convergencia de la humanidad con la tecnología, facilitando de manera óptima la forma y calidad de vida de las personas" (Saint, 2015). El internet de las cosas (IoT) es una tecnología en constante evolución y desarrollo a nivel mundial que busca ofrecer facilidades para mejorar la calidad de vida de las personas. Actualmente IoT ha sido implementada en áreas como la salud, el transporte, el hogar, entre otros.

Desde un punto de vista de investigación y desarrollo ofrece gran variedad de oportunidades debido a la diversidad de áreas en las que se puede implementar. Sin embargo es necesario un estudio en donde se analice la integración de conocimientos aplicados en la temática, de esta manera que se determine una adaptación a diferentes ámbitos sociales que garanticen una oportunidad de mejorar la calidad de vida de las personas (Shorter, 2014).

3.1 Internet de las cosas (IoT)

El internet de las cosas se refiere a la interconexión digital de una variedad de objetos cotidianos, la idea fundamental es que todos los elementos se conecten a Internet, como

refrigeradores, lámparas, cerraduras, accesorios de vestir, partes del automóvil, implantes cardiacos, entre otros. El objetivo es facilitar el manejo de todos estos dispositivos, ya sea entre ellos o con personas, consolidándose como una automatización en los diversos campos y áreas del quehacer humano.

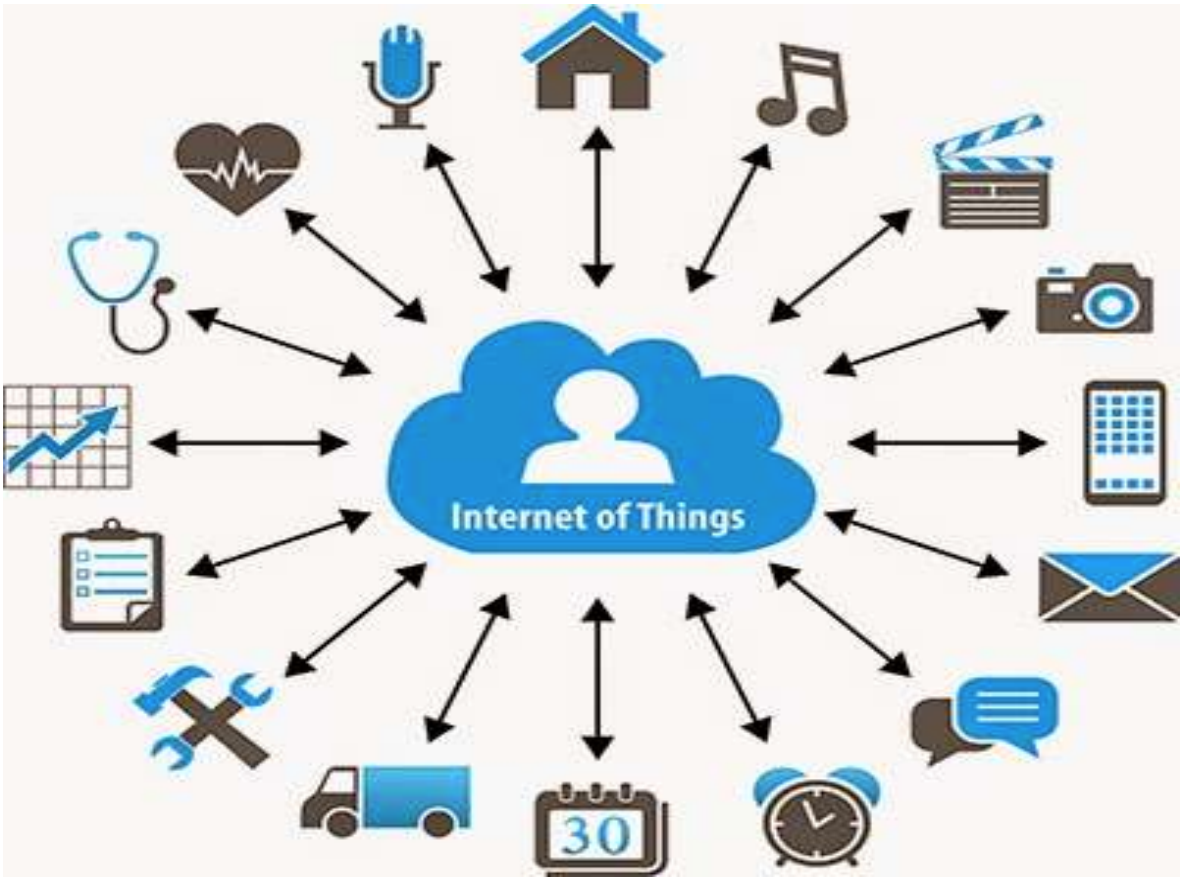
El objetivo de IoT es brindar un valor agregado que permita una convergencia de diferentes tecnologías, para generar soluciones que integren diferentes características y logrando un mayor control sobre las cosas. Una de las principales razones para el desarrollo de IoT es la constante interacción que el usuario busca con la tecnología, con la visión de ir más allá de los escenarios móviles y evolucionar a la conexión e incorporación de la inteligencia en las cosas (Ren Duan, 2011) (Spring, 215).

El nuevo ámbito tecnológico estará alejado de un escritorio, IoT permite que cada objeto se encuentre en una red, en otras palabras la idea general es que los objetos tengan la posibilidad de conectarse a una red para comunicarse con otros dispositivos y de esta manera poder cumplir con los diferentes proyecciones que se tienen hacia un entorno automatizado (Jayavardhana Gubbi a, 2013).

Así, a través de diversos protocolos y aplicaciones, en un futuro no muy lejano habrá más dispositivos conectados al ciber espacio o a la nube que personas con vida. Teniendo en cuenta como ejemplo que cada persona se encuentra rodeada de al menos unos cien objetos.

Algunas de las empresas pioneras a nivel mundial en el tema IoT son Google, Nidia, Panasonic, Huawei, IBM, entre otras. Estas calculan que para el año 2020 existirán por lo menos entre 26.000 y 30.000 millones objetos conectados a internet en todo el mundo y por supuesto integrando las aplicaciones que el internet de las cosas brindará (Saint, 2015).

Imagen 1 Internet de las cosas



Fuente: Revista Española de Electrónica, Ediciones técnica REDE, 2015

El IoT permite estimular un desarrollo económico y social, ampliando los servicios que se puedan prestar mediante la masificación y desarrollo de la tecnología (Imagen 1). El uso de nuevas tecnologías facilita los procesos de comunicación dentro de la sociedad, por lo cual se resalta la importancia de estudiar, analizar y plantear posibles oportunidades de desarrollo que generen la posibilidad de establecer nuevas ideas de negocios (Porkodi, 2014).

El potencial de IoT en el sector económico es amplio, hasta el punto de lograr generar a nivel mundial un impacto económico entre $2.7 y $6.2 trillones de dólares estimados para

el 2015 (Saint, 2015). Estas cifran representan la oportunidad de un desarrollo tecnológico bastante sofisticado, que garantice la mejora en la calidad de vida de las personas, sin embargo, genera algunas complicaciones o fallos entre los cuales se nombran: seguridad frente a la vulnerabilidad en las redes, falta de innovación y el sedentarismo en la vida de las personas (Heng Li, 2011).

Es ahora cuando es necesario aprovechar de una manera óptima la nueva tendencia del internet de las cosas, para encontrar fortalezas que busquen conocer los requisitos de una automatización del entorno, garantizando una mejora en la calidad de vida frente a un mundo tecnológico que ya empieza de manera exponencial a difundirse a nivel mundial (Stefan Nastic, 2014).

El IoT pretende conectar todo dispositivo que cuente con una conexión a internet, en todo momento y en todo lugar, mediante dispositivos sensores tales como RFID (Radio Frequency Identification) con el fin de lograr el reconocimiento inteligente y gestión de red (CÉSAR ANDRÉS GAVIRIA CUEVAS, 2014).

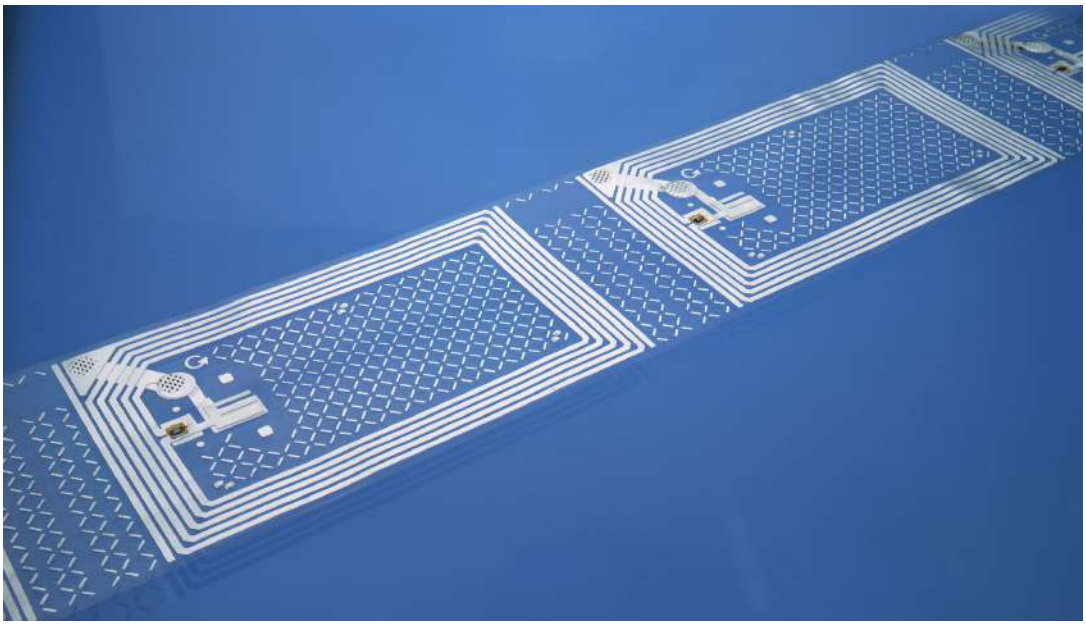
3.2 Tecnología RFID

En el año de 1998 Sarma y David Brock provenientes del Massachusetts Institute of Technology (MIT) crearon las etiquetas de identificación Rifad. Esta identificación por radiofrecuencia permiten acceder remotamente desde una serie de etiquetas o tags, que se encuentran pegados o adjuntos a cada uno de los elementos a los que se les quiere hacer un seguimiento. Cuando estas etiquetas se encuentran en cada uno de los objeto a identificar esta información puede ser almacenada y procesada por los sistemas de gestión. Sin embargo esta tecnología no es novedosa ya que en la segunda guerra mundial era usada por

los británicos con el fin de ubicar sus aviones y de esta manera no realizar lo que se conoce como fuego amigo.

El desarrollo de RFID fue novedoso por su bajo costo y por garantizar una conexión a internet, el principal objetivo de este desarrollo, con el fin de sustituir el código de barras UPC (Universal Producto Code) por el EPC (Electronic Product Code). Entonces se realizaron múltiples investigaciones por diferentes institutos, entre los cuales estaban: Auto-ID Center, siete universidades de cuatro continentes y EPCglobal, en el año 2003 anuncian las tecnología llamada RFID y normas realizadas para poder trabajar con la red EPC, estas etiquetas se pueden observar en la imagen 2 su finalidad es garantizar el flujo de información por la red (Stefan Nastic, 2014).

Imagen 2 Sensor RFID



Fuente: Weinstein, Ron, RFID: A Technical Overview and Its Application to the Enterprise

El funcionamiento de RFID se basa en tres elementos esenciales:

1. Ubicar las etiquetas en el objeto a seguir. Las etiquetas pueden ser pasivas o activas. Las pasivas son utilizadas para elementos u objetos de menor costo ya que simplemente constan de una antena que recibe de forma pasiva la energía que envía el lector para emitir la información almacenada en las etiquetas, tienen un alcance muy limitado aproximadamente de uno a tres metros. Mientras las activas tienen una batería que les permite durar varios años y su precio es mayor, permite emitir a varios metros (Porkodi, 2014).
2. Los lectores o sensores de estas etiquetas tienen la tarea de leer la información y procesarla adecuadamente para enviarla al tercer elemento importante que es el middleware.
3. El Middleware es la pieza de software que realiza un procesamiento de la información para ser analizada, para luego enviarla a cada uno de los elementos de ese escenario.

Las aplicaciones de la tecnología RFID abarcan un amplio campo, sin embargo, es importante hablar de los beneficios relacionados con la productividad de lectura de los elementos frente a una lectura tradicional como el código de barras. La Productividad de lectura ayuda con un control adecuado a cada uno de los dispositivos que tengan una etiqueta. Otra de sus principales características es que genera una visibilidad de suministro que hace que se pueda tener más información inmediatamente (Stefan Nastic, 2014).

De esta tecnología vale la pena resaltar la reducción en la pérdida de información, ya que reduce la probabilidad de error humano. Al hablar de RFID es necesario conocer el término

de EPC, (Electronic Product Code) que permite de alguna manera la comunicación entre los objetos.

El EPC es un componente esencial de IoT, que se encuentra soportado y apoyado en un sistema científico-tecnológico, que busca nuevos desarrollos para acoger las diferentes aplicaciones. Este término se puede clasificar en dos grandes conceptos: los códigos EPC y las redes EPC.

Los códigos EPC: Son los códigos de producto electrónico, que contiene toda la información que se va a emitir y compartir con las diferentes etiquetas RFID. Un código es un número o un identificador electrónico específico para cada uno de los productos (Gill, 2013).

La red EPC: Permite la interacción de diferentes actores, con el objetivo de intercambiar información específica sobre cierto producto. En cada etiqueta RFID únicamente reside el identificador, y toda la información asociada con este identificador se encuentra en la red EPC, incluyendo por ejemplo toda la información de fábrica, escalabilidad del producto, distribuidor, entre otros (Gill, 2013).

3.3 Sistemas físicos del ciberespacio

El concepto del internet de las cosas y el de los sistemas físicos del ciberespacio se encuentran relacionados. Helen Gill de la Fundación Nacional de Ciencia de los Estados Unidos (Por sus siglas en ingles NFS – United States National Sciencie Foundation), sugirió la idea en el año 2013 “los ciber sistemas físicos son sistemas físicos, biológicos y artificiales cuyas operaciones están integradas, supervisadas y controladas por un núcleo,

cuyos componentes están conectados en red en todos los estratos" (Gill, 2013), es aquí donde definía que todos los objetos físicos deberían estar controlados sistemáticamente, de modo que, la informática juega un papel importante, ya que es la parte fundamental de la operación de todos estos sistemas interconectados entre sí.

Este concepto fue acogido rápidamente por varios organismos e instituciones de los Estados Unidos entre los cuales cabe resaltar a Nacional Institute of Standards and Techonology (NITS) y Georgia Insitute of Techonology, los cuales empezaron a realizar proyectos de investigación permitiendo una rápida evolución y desarrollo de estos sistemas del ciberespacio (Heng Li, 2011).

La idea de estas instituciones es que "La informática está profundamente incrustada en todos los componentes físicos e incluso posiblemente en los materiales. El núcleo informático de un sistema anidado que suele exigir respuestas en tiempo real y en la mayoría de los casos esta distribuido" (Gill, 2013), esta idea se basa en la necesidad que cada uno de los elementos interactúe entre ellos en tiempo real, de modo que el tiempo no sea percibido, permitiendo una interacción adecuada con cada sistema.

La revolución de los sistemas físicos es una tecnología en constante desarrollo, que es principalmente utilizada en ciudades inteligentes, mejorando el factor económico de cada ciudad que lo implemente. Todo esto podría generar una nueva revolución industrial encaminada a un internet de las cosas, con variedad de servicios y datos.

3.4 Redes de sensores inalámbricos (WSN)

Los recientes avances tecnológicos en circuitos integrados de baja potencia y las comunicaciones inalámbricas han puesto a disposición dispositivos de tamaño reducido con capacidad para comunicarse en etapas de detección. El tamaño de estos dispositivos ha mejorado la capacidad de utilizar sensores inteligentes que permiten la recolección de información, procesamiento, análisis y control de la información (Jayavardhana Gubbi, 2013).

La tecnología RFID es casi lo mismo que los nodos de sensores inalámbricos, sin embargo, estos últimos tienen capacidad de procesamiento y almacenamiento menor. Los retos planteados para el desarrollo y mejoramiento de estos sensores son la reducción de tamaño y la mejora en el procesamiento , presentando un potencial de evolución.

Los datos del sensor son compartidos entre los demás sensores y se envían a un sistema distribuido o centralizado quien es el encargado de analizarlos. Existen varios componentes que conforman una red de sensores inalámbricos: WSN hardware, pila de comunicación, WSN Middleware y agregación de datos.

a. WSN Hardware: Son interfaces de sensores que tienen la tarea de ser fuente de alimentación en la recepción de datos y de comunicarse mediante espectro electromagnético de manera que sean más versátiles (Jayavardhana Gubbi a, 2013).
b. La pila de comunicación: Es la encargada de la comunicación entre los diferentes dispositivos WSN. Puede configurarse en distintas topologías según el diseño, enrutamiento y la posibilidad de escalabilidad de la red. Transmite los datos con el objetivo de ser analizados en una capa posterior (Jayavardhana Gubbi a, 2013).

c. WSN Middleware: Es un mecanismo que combina la infraestructura de los sistemas físicos con los sensores de red para facilitar el acceso a los recursos de las diferentes aplicaciones (Jayavardhana Gubbi a, 2013).
d. Agregación de datos: Es la encargada de brindarle seguridad a la red y de esta manera garantizar la fiabilidad de los datos obtenidos por los sensores (Jayavardhana Gubbi a, 2013).

3.5 Near Field Communication

Near Field Communication (NFC) o comunicación de campo cercano, es un conjunto de estándares principalmente para los teléfonos inteligentes y otros dispositivos móviles, su finalidad es permitir el establecimiento de comunicación con los otros dispositivos simplemente tocándose entre ellos o reuniéndolos a una distancia muy pequeña (Porkodi, 2014).

Actualmente, los dispositivos NFC se encuentran implementados con éxito en los sistemas de pago de tarjetas de crédito y tarjetas inteligentes, los cuales pueden ser utilizados en diferentes ámbitos mostrando un gran desempeño y de esta manera mejorar los medios de pago existentes (Saint, 2015).

3.6 Sensores y teléfonos móviles

Los teléfonos móviles inteligentes son una parte fundamental de la vida cotidiana de muchas personas. Gracias a su uso generalizado, las redes móviles juegan un papel importante en la masificación de nuevas tecnologías. Hoy en día, los teléfonos móviles no

son solo un dispositivo para poder realizar llamadas, estos están equipados para poder ejecutar funciones de datos, textos y hasta video streaming (Porkodi, 2014).

En la actualidad, la combinación de sensores con los teléfonos móviles ofrece varias aplicaciones, una de ellas importantes es que pueden funcionar como receptor y transmisor de datos recolectados por sensores móviles, detectando actividades sencillas como: reconocimiento de movimiento, detección de su entorno, hasta el reconocimiento de olores, etc. (CÉSAR ANDRÉS GAVIRIA CUEVAS, 2014).

3.7 Seguridad y privacidad en las redes

La seguridad es y continuará siendo una preocupación importante, tanto para los desarrolladores como para los usuarios. Debido a que la red está compuesta por muchos dispositivos y cosas conectadas a esta, se puede presentar una vulnerabilidad en cuanto a la seguridad que podría afectar masivamente a los usuarios (Dr. Peter Friess, 2012). Un sistema puede ser atacado de muchas maneras, algunos ejemplos pueden ser la desactivación de la disponibilidad de la red, generación de datos erróneos en la red, o incluso el acceso a información personal de los usuarios.

Es imposible imponer una privacidad adecuada con un mecanismo el cual no pueda ser vulnerado. De este modo la seguridad se convierte en una gran preocupación haciendo patente la necesidad de incorporar medidas de seguridad adecuadas dependiendo de la aplicación, mediante diferentes técnicas de desarrollo (J. Domingue, 2013). Este tema se profundiza en el capitulo 6, ya que se considera una de las áreas de investigación y desarrollo alrededor de IoT.

3.8 Calidad de servicio

El IoT es probablemente uno de los avances mas importantes de los últimos años, la capacidad de operar entre protocolos de comunicación donde físico y virtual tienen identidad y atributos que caracterizan la red de información. Las cosas u objetos inteligentes son participes activos en los procesos de negociación permitiendo comunicarse entre sí mediante el intercambio de información detectada por el medio ambiente.

En esta perspectiva, es necesario definir la calidad de servicio en factores necesarios para satisfacer los requisitos de cada una de las aplicaciones. Diferentes plataformas en la nube proporcionan un marco para el desarrollo a gran escala de IoT que dependen de la recolección compleja de datos adquiridos por los sensores y dispositivos inteligentes. Sin embargo, los requisitos para cumplir una calidad de servicio adecuada están parame trizados por unos factores.

La calidad de servicio de las aplicaciones de IoT se mide a partir de factores primarios, como por ejemplo, el rendimiento y el aprovechamiento del ancho de banda. Es necesario brindar garantías de calidad de servicio debido a las limitaciones que se tienen en la asignación de recursos y la capacidad de gestión de los medios de transmisión.

La calidad de servicio depende principalmente de CloudComputing que es el almacenamiento en la nube, esta es una área de investigación bastante compleja, que cada vez necesitan más atención por la cantidad de datos, elementos y herramientas que se disponen allí. Esto lleva a desarrollar un enfoque controlado para servir a los diferentes tráficos que se pueden presentar en la red y de esta manera tener la garantía de poder asignar los recursos y hacer una gestión adecuada de ellos en la red (R. Johnstone, 2008).

Desafíos surgen con respecto a la utilización óptima de los recursos disponibles, por ejemplo, el consumo de energía resultante de la presentación de informes en la lectura de los sensores de cualquier dispositivo físico. Siguiendo otros factores para determinar una métrica se puede encontrar la optimización y autogestión, que prácticamente especifican el diseño de cualquier arquitectura en general describiendo detalladamente parámetros relacionados con el nivel físico (sensores), nivel de red y nivel de aplicación.

Por tal motivo, la calidad de servicio se encarga de gestionar las métricas y requisitos generales para la recolección de datos por medio de los sensores y la optimización de los recursos centrados en la aplicabilidad en el medio ambiente para generar un monitoreo de cualquier tipo de aplicación y garantizar el correcto y óptimo desarrollo de esta.

4 PROTOCOLOS

Los protocolos de comunicación entre dispositivos IoT tienen un papel importante en el despliegue de las aplicaciones. Los protocolos son la base fundamental para generar una comunicación con el entorno mediante la información que reciben los sensores. Se han propuesto varios conjuntos de mecanismos MAC (Medium Access Control) o por sus siglas en español control de acceso al medio, este mecanismo se basa en una serie de algoritmos que se encargan de realizar la comprobación de los distintos dispositivos que interactúan con el entorno (Porkodi, 2014).

El conjunto de mecanismos MAC utiliza TDMA (Acceso Múltiple por división de tiempo) que es una técnica con el fin de transmitir diferentes señales digitales, para ello el ancho de banda del medio es asignado a cada canal durante un determinado periodo o intervalo de tiempo, CSMA (Carrier Sense Multiple Access) para evitar colisiones se escucha al medio de transmisión y de esta manera se determina si existe la presencia de una portadora en el canal y de esta manera evitar que varios host hablen al mismo tiempo y por ultimo FDMA (Acceso Múltiple por División de Frecuencia) es una multiplexación realizada dividiendo el espectro en canales que se encuentren disponibles a bandas de diferentes frecuencias y transmitir de esta manera simultáneamente por un medio de transmisión; sin embargo, todos estos requieren circuitos adicionales en los nodos para generar su respectivo procesamiento (Porkodi, 2014).

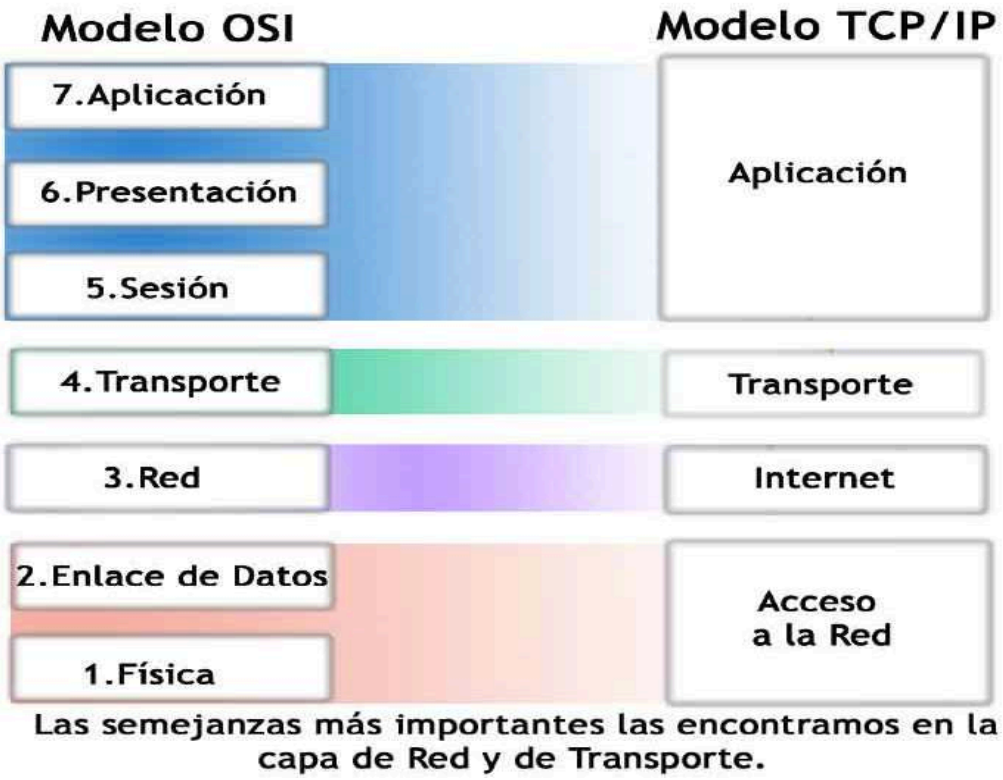
Para la descripción de los protocolos fue necesario la adaptación de un modelo, para este caso el modelo a seguir fue TCP/IP.

4.1 Modelo TCP/IP

El modelo TCP/IP describe un conjunto de especificaciones para el diseño y la implementación de protocolos de red, para permitir que cualquier dispositivo se pueda comunicar en la red. TCP/IP tiene la ventaja de garantizar una conexión de punto a punto especificando datos transmitidos, direccionados, enrutados y recibidos por el destino.

Este modelo tiene la ventaja de estar seccionado en capas o niveles las cuales facilita la agrupación funciones. Las capas o niveles de TCP/IP se encuentran jerarquizadas de la siguiente manera:

Imagen 3 Capas de modelo TCP/IP



Fuente: Universidad de Granada, Departamento de ciencias de la computación

El modelo TCP/IP consta de 4 capas, cada cuna de ellas debe ocuparse exclusivamente de su nivel inferior como se observa en la imagen 3, a quien se le solicita cada uno de los servicios que requiera y del nivel superior quien es el que devuelve los resultados.

- Capa de aplicación: La capa de aplicación debería incorporar parámetros de las capas de sesión y presentación del modelo OSI. Esta capa es la encargada de manejar todo lo relacionado con la representación, codificación y control de dialogo.
- Capa de transporte: Se asimila a la capa de transporte del modelo OSI. Se encarga de efectuar el transporte de los datos desde el dispositivo de origen hasta el destino.
- Capa de internet: Se asimila a la capa de red del modelo OSI. Encargada de identificar el tipo de enrutamiento que existe entre una o mas redes.
- Capa de acceso al medio: Asimilable a la capa de enlace de datos y capa física del modelo OSI. Encargada del direccionamiento físico, acceso al medio y la topología de la red y las conexiones globales.

4.2 CAPA DE INTERNET

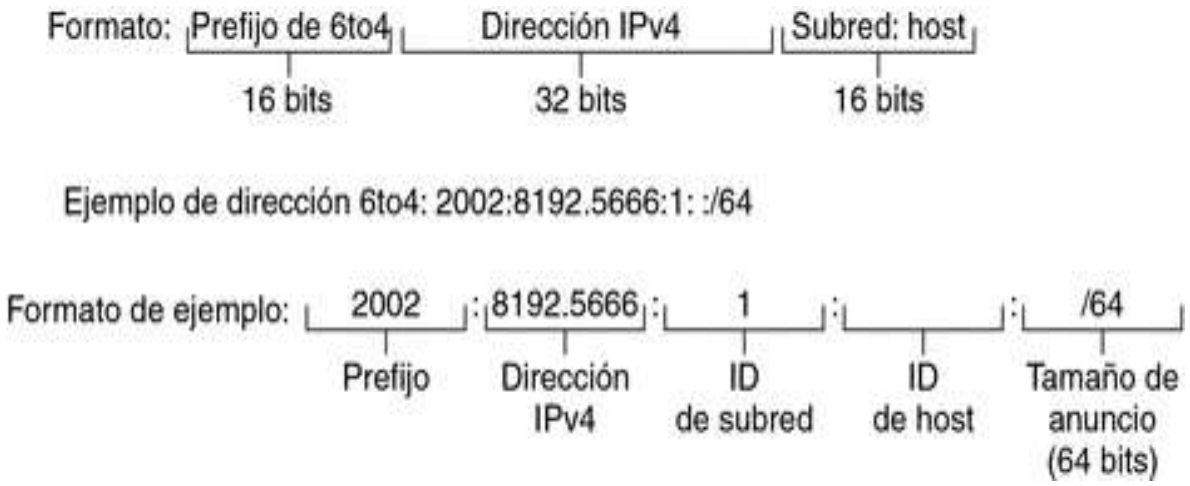
4.3 IPv6

El protocolo de internet 6 (IPv6) (RFC 6275) es el protocolo mas reciente implementado hoy en día, este aumenta considerablemente el número de direcciones de internet y de esta manera la capacidad de procesar y analizar grandes volúmenes de datos, este protocolo

tiene la capacidad de poderse comunicar prácticamente con todos los dispositivos existentes en el mundo ya que el espacio de direcciones es extremadamente grande (Porkodi, 2014).

Desde un principio el interés de los diseñadores de este protocolo era que las direcciones fueran mas extensas y de esta manera mejorar la jerarquía sistemática y la eficiente asociación de rutas. El tamaño de una subred de IPv6 es de 2^64 (con mascara de subred de 64 bits) de esta manera se garantiza un número ilimitados de host en cada subred como se observa en la siguiente imagen, en la cual se ve el formato de la dirección IP, que consta de: un prefijo de identificación, la dirección de IP, el identificador de subred y host.

Imagen 4 Formato de direcciones IPv6



Fuente: Jordi Palet, ConsulIntel, Consultores integrales de Telecomunicaciones.

La ventaja de este protocolo es que los nodos pueden autoconfigurarse en la red de una manera instantánea, ya que cuando se conecta cualquier dispositivo en la red este envía un mensaje de ICMPv6, el cual envía una solicitud al router pidiendo cada uno de los parámetros de configuración. En caso de que la implementación no use ICMPv6, se puede hacer uso de DHCPv6.

4.4 ICMPv6

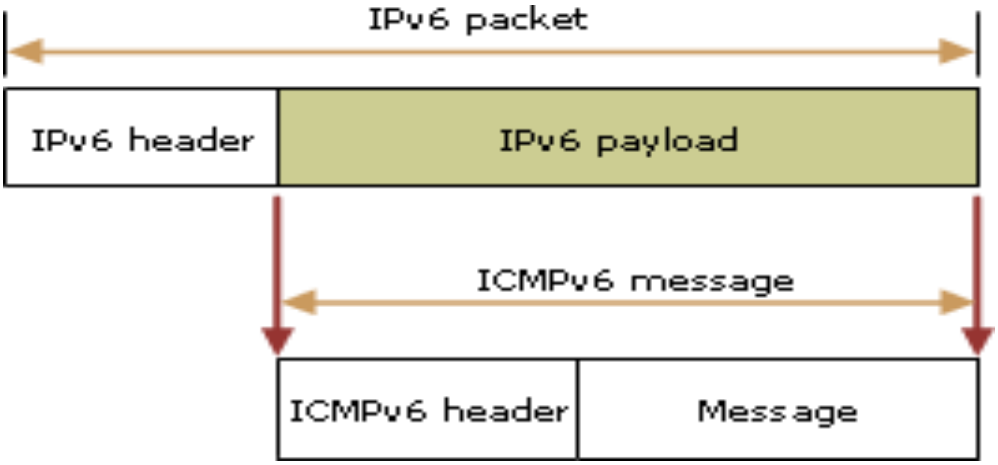
ICMPv6 (Internet Control Message Protocol 6) (RFC 6145) es una parte integral de IPv6, es la necesaria para complementar las implementaciones que tiene IPv6. ICMPv6 combina funciones de diferentes protocolos, entre los cuales se encuentran:

- ICMP (Internet Control Message Protocol) para IPv4.
- IGMP (Internet Group Managment Protocol).
- ARP (Address Resolution Protocol).

Introduce algunas simplificaciones mediante la eliminación de mensajes obsoletos o que ya no se encuentran en uso. Este protocolo se utiliza para detectar errores de información en los paquetes, realizando análisis a los vecinos y de esta manera detectar estos errores y posteriormente informando por multidifusión a cada uno de dispositivos de la red.

Los mensajes ICMP se subdividen en dos tipos de clases: los mensajes de error y los mensajes de información. Todos estos mensajes se transportan en un paquete IPv6 en el cual la cabecera siempre se encuentra presente con la información actualizada. En la siguiente imagen 5 se muestra un mensaje ICMP en un paquete IPv6.

Imagen 5 Funcionamiento ICMPv6



Fuente: IPv6 Addressing and Basic Connectivity Configuration Guide, Cisco

Radio Link Protocol (RLP), consiste en una petición automática que se utiliza principalmente en las comunicaciones inalámbricas. La mayoría de las interfaces inalámbricas tienen un porcentaje de 1% de perdida de paquetes, este es un porcentaje bastante tolerable, sin embargo se desea mejorar la fiabilidad de las redes que transportan datos TCP/IP.

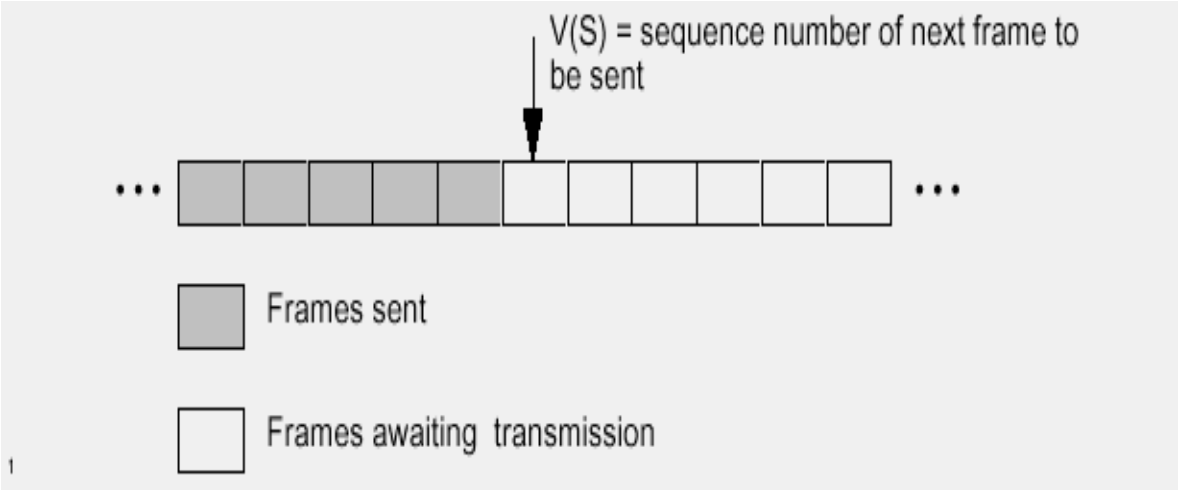
4.5 CAPA DE ACCESO AL MEDIO

4.6 RLP

RLP (RFC 887) esta diseñado para crear un destino orientado a mantener estable la topología de la red, ya que contiene las rutas de cada uno de los nodos teniendo en cuenta que todos serán gobernados por un nodo raíz, en este caso este nodo será el servidor web. Por lo tanto los nodos consideran un objetivo minimizando o maximizando los recursos de

la red dependiendo de la aplicación requerida o las métricas de enrutamiento, con el fin de garantizar un mejor coste en cuanto a la ruta elegida (Sheeraz A. Alvi, 2015).

Imagen 6 Funcionamiento RLP



Fuente: Radio Link Protocol (RLP) for data and telematic services on the Mobile Station, ETSI

Tal como se denota en la imagen 6, RLP utiliza tres paquetes ICMPv6 para el enrutamiento de la señalización, mientras que la creación y mantenimiento de la tabla de enrutamiento la realiza el servidor o el nodo de raíz, el cual con anterioridad sabe su destino y por medio del protocolo se puede garantizar la ruta de menor coste.

RLP no puede pedir la interfaz para proporcionar adecuadamente el tamaño de lo que conformará la carga útil, en cambio el planificador si tiene la capacidad de determinar el tamaño del paquete. Sin embargo, es un protocolo bastante flexible ya que tiene la capacidad de transmitir durante el desvanecimiento de la señal inalámbrica ya que proporciona una pérdida de tan solo 1%, teniendo una memoria temporal para almacenar la última información enviada (Sheeraz A. Alvi, 2015).

Con el objetivo de reducir costos y utilización de los recursos normalmente los nodos interesados se comunican con el objetivo de transmitirse entre ellos paquetes mas pequeños con una secuencia enumerada y de esta manera se tenga el control del paquete total al momento de codificar la señal original.

RLP en ocasiones tiene acuse de recibo y en otras no, eso depende principalmente de la calidad de la conexión establecida, cuando se recibe un segmento fuera de orden el receptor envía el acuse de recibo con la necesidad de garantizar el orden del paquete y de esta manera evitar una latencia ineficiente para de esta manera poder retransmitir el mensaje en caso de que fuera necesario (Sheeraz A. Alvi, 2015).

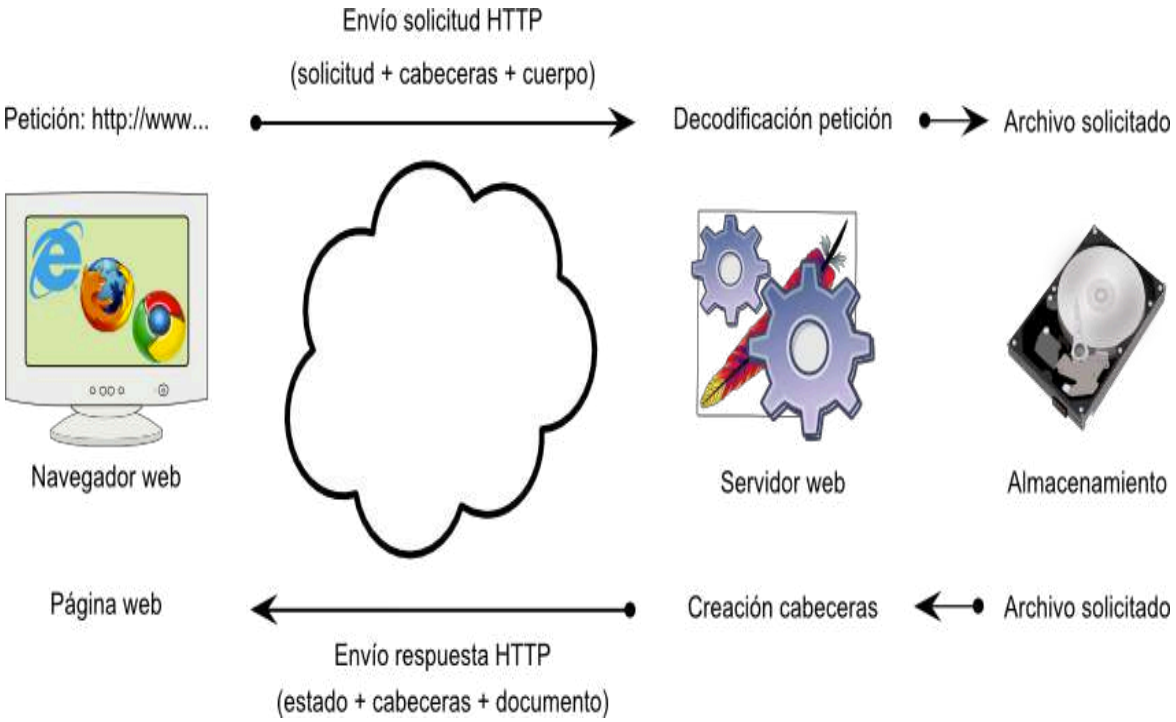
4.7 CAPA DE APLICACIÓN

4.8 Protocolo HTTP

Hypertext Transfer Protocol (HTTP) (RFC 2817), es un protocolo de aplicación, para sistema de información hipermedia distribuidos, es la base para la comunicación de datos www (World Wide Web). Funciona como un protocolo de petición y respuesta en los modelos básicos de cliente y servidor. Un ejemplo es, un navegador puede ser el cliente y cualquier aplicación que se ejecuta en un sitio web puede ser el servidor. El cliente envía la petición correspondiente http al servidor, este ofrece cada uno de sus recursos como archivos HTLM (HyperText Markup Language) y demás contenidos, devolviendo una respuesta al cliente que contiene toda la información sobre la solicitud y el cuerpo del mensaje en si (Berners-Lee, 2010).

El protocolo HTTP está diseñado para permitir que cada uno de los elementos de red intermediarios intercedan con el objetivo de mejorar la comunicación entre el cliente y el servidor. Esto debido a los sitios donde se encuentra un alto tráfico que benefician a los servidores cache que ofrecen el mismo contenido que los servidores originales, garantizando una respuesta a mayor velocidad reduciendo considerablemente la latencia.

Imagen 7 Funcionamiento de las peticiones HTTP



Fuente: Francisco Prieto Donate, Protocolo HTTP

Cada uno de los recursos HTTP se encuentran y se identifican claramente en la red con una localización especifica para que de esta manera la asignación de recursos sea adecuada, el uso de esquemas que identifiquen la asignación de recursos forman una organización adecuada para la respuesta de cada una de las peticiones de cada documento interrelacionados por hipertexto (Berners-Lee, 2010).

Los navegadores cache puede acceder a los recursos web y de alguna manera reutilizarlos para de esta manera reducir el tráfico en puntos calientes donde puede generarse cogestión, por esta razón existen servidores proxy HTTP con el objetivo de facilitar la comunicación de los clientes sin una dirección global, simplemente toda la información se encuentra almacenada en ellos ya que previamente estos se comunican con los servidores externos (Berners-Lee, 2010).

Este protocolo es bastante útil en IoT, debido a las nuevas tecnologías que se implementan entre las cuales la mas reconocida es la domótica, se necesita claramente la necesidad de requerir hipertexto en la web para facilitar diferentes tareas requeridas por los usuarios. Sin embargo, se están manejando actualizaciones de http por la empresa google, quien cuenta con una mejora es su ultimo protocolo llamado SPYDY que es bastante similar al http en cuanto a comunicación.

4.9 Protocolo de Movilidad

No existe con claridad un protocolo de movilidad en IoT utilizando IPv6, es decir los paquetes destinados a un nodo móvil (MN) no podrían ser enviados cuando se mueve fuera de la red original o de la red en la cual esta su asignación IP. De hecho, el MN transmite los paquetes a la dirección IP anterior que en este caso ya estaría obsoleta.

De esta manera para poder continuar con la comunicación sin importar sus movimientos, un MN obtendrá una nueva IPv6 dependiendo de la red actual en la cual se encuentre. Sin embargo, esto no será suficiente para tener una comunicación continua y estable. Por esta razón se restablece una sesión con el MN en la cual se encuentran sus últimos datos

almacenados pensando en los paquetes que pueden ser transmitidos por otro nodo (Amel Achoura, 2015).

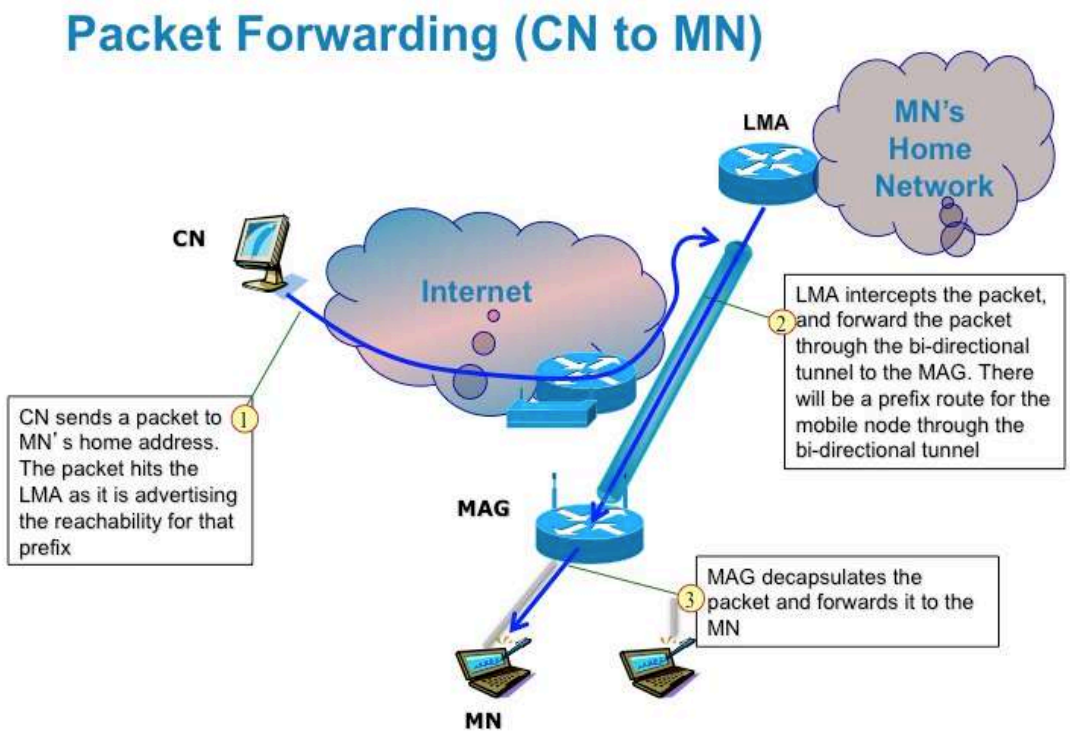
Para cualquier desarrollador e investigador de IoT esto se convirtió en un problema a solucionar, para ello se ha diseñado IPv6 para mejorar considerablemente la movilidad llamado MIPv6 y de esta manera sin importar en la red que se encuentre haya una comunicación estable. Principalmente utilizado en las redes domesticas en donde se crearan diferentes redes con el objetivo de mejorar la interacción con los diferentes dispositivos en su interior.

4.10 MIPv6

Mobile IPv6 (MIPv6) (RFC 4225) es un protocolo desarrollado como un subconjunto del protocolo de internet versión 6 (IPv6) para apoyar las conexiones móviles. MIPv6 es una actualización de la IETF (Internet Engineering Task Force) Mobile IP estándar (RFC 2002), diseñado para autenticar dispositivos móviles conocidos como Mobile Node (MN)

Cuando MN se mueve de cualquier de una red doméstica a una red visitada , se obtiene una nueva dirección IPv6 temporal dentro de esta nueva red, entonces el MN indicará a su servidor de raíz que su ubicación ha cambiado y transmite su nueva dirección temporal. Esto se puede realizar por medio de un túnel bidireccional IPv6 que se establece entre el MN y su servidor (Amel Achoura, 2015).

Imagen 8 Funcionamiento MIPv6



Fuente: Courtesy of Youn-Hen Han Korea, University Of Technology

El servidor re direccionará el tráfico, sin embargo, el nuevo nodo de control (CN) de la nueva red interceptará todos los paquetes con el objetivo de garantizar la comunicación entre estos. Desde un punto de vista externo no se generará ningún cambio ya que la transmisión de paquetes permanecerá idéntica independientemente de la ubicación del MN.

Aunque este protocolo de movilidad sea bastante popular y sea fácil de implementar, tiene algunas limitaciones en cuanto a las detección de algunas conexiones o la pérdida de paquetes generadas por los retardos, todo esto se debe a:

- Falta de comunicación en la detección de la llegada de un MN en la nueva red.
- Tiempo para la adquisición de la dirección temporal.

- Tiempo de comunicación en el almacenamiento de la dirección temporal.

Para mejorar considerablemente estos problemas se desarrollaron algunas soluciones bastantes practica:

- Traspasos de protocolo rápido para MIPv6 por medio del protocolo (FMIPv6) el cual tiene el objetivo de reducir la latencia, para ello el MN puede solicitar información acerca de los puntos de acceso que lo rodean y de esta manera anticipar su llegada a la nueva red (Amel Achoura, 2015).
- Jerarquía móvil (HMIPv6) la cual es también una solución enfocada al MN, reduce la latencia por medio de una "entidad" que actúa como nodo de control y por lo tanto enmascara el tráfico de señalización dentro del futuro dominio y así su latencia se minimizará considerablemente (Amel Achoura, 2015).
- Proxy móvil (PMIPv6) es un protocolo de apoyo a la movilidad de la red, el enfoque de este protocolo se encargará de toda la señalización para el MN el cual limita la comunicación en las redes que pertenecen al mismo dominio de proxy (Amel Achoura, 2015).
- La movilidad de soporte básico de red (NEMO) es un protocolo que considera la movilidad completa que enfoca su gestión en la comunicación con los routers inalámbricos y transmite diferentes mensajes de señalización en nombre de la red (Amel Achoura, 2015).

Estas anteriores soluciones permitieron mejorar las limitaciones que se presentaban en cuanto a la movilidad. Para ello se debe optimizar el retardo de transferencia, la detección de movimiento y el coste de señalización para reducir el consumo de energía y preservar las

actuaciones de los nodos, la unión de todos los protocolos nombrados en este capítulo brindan una solución que ayuda a la comunicación (Amel Achoura, 2015).

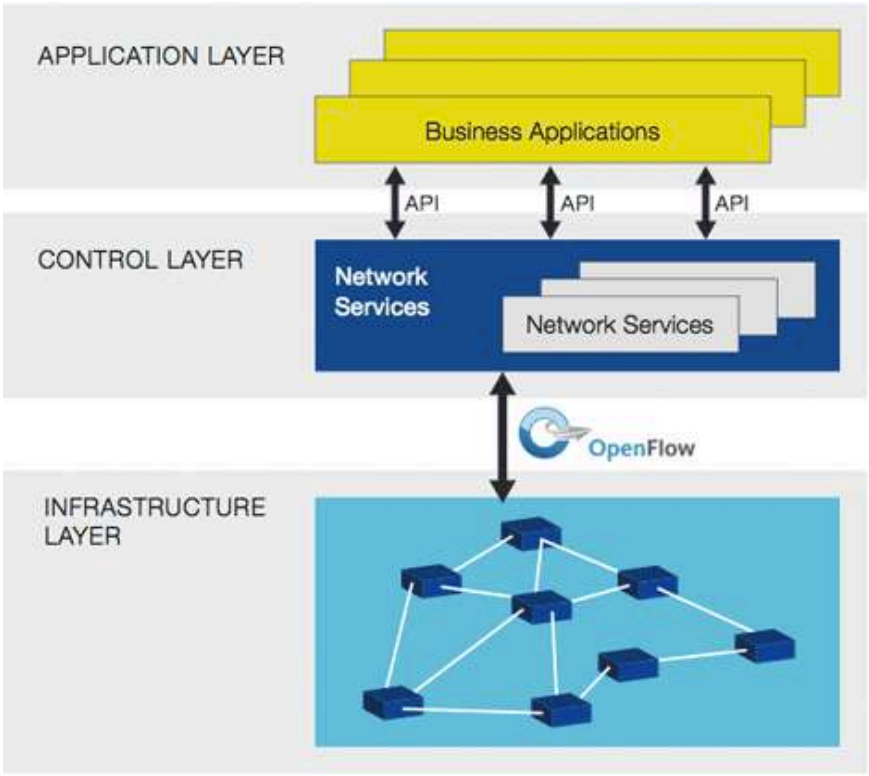
4.11 ARQUITECTURA COMO APOYO A LOS PROTOCOLOS

4.12 SDN

Software Defined Networking (SDN) aunque no es un protocolo sino una arquitectura de red, se tiene en cuenta debido a su estrategia para aumentar la funcionalidad de la red, reduciendo costos, complejidad del hardware y permitiendo la una investigación innovadora. La arquitectura SDN tiene tres capas: la capa de infraestructura que consiste en los dispositivos de red (Conmutadores, routers, switches virtuales, puntos de acceso inalámbricos, etc.), una capa de control que consta del controlador SDN y una capa de aplicación para configurar el SDN (Control de acceso, el tráfico, seguridad, gestión de red, etc.) (FLAUZAC Olivier, 2015).

Una característica importante de la arquitectura SDN es la capacidad que tiene para ampliar el perímetro de seguridad de los dispositivos, mediante el establecimiento de políticas de seguridad que siguen unos parámetros de confiabilidad. Todo lo anterior se realiza gracias al controlador SDN que construye una gráfica de la red mundial mediante los dispositivos intermedios para establecer una conexión segura (FLAUZAC Olivier, 2015).

Imagen 9 Arquitectura SDN



Fuente: Introduction to Software Defined Networks (SDN) and its relevance in the DC, CISCO

Por otra parte, las amenazas de seguridad son otro inconveniente, como la denegación de servicio (DoS), si un atacante compromete el controlador SDN, entonces él tiene el control total sobre la red y esto representa un riesgo potencial para toda la red. Además, los fallos de hardware y software pueden ocurrir con un único sistema de control. Sin embargo al tener varios sistemas de control ofrece confiabilidad y tolerancia a fallos mejorada, ya que si uno de los controladores SDN cae el otro puede tomar el control para evitar el fracaso del sistema.

5 ENERGÍA

Uno de los factores mas importantes y que inquieta a la sociedad es la conciencia ambiental con respecto al dióxido de carbono y sus efectos, por esta razón ha inspirado a cada uno de los departamentos TIC del mundo a realizar investigación para de esta manera asegurar una baja potencia y un funcionamiento ecológico de los sistemas de comunicación con el fin de minimizar las emisiones de huella de carbono (Wade Trappe, 2015).

Por esta razón la comunidad científica se ha centrado específicamente en la minimización de las emisiones de dióxido de carbono y la energía disipada por las redes inalámbricas, para de esta manera garantizar el nuevo término de la comunicación verde. Sin embargo, el tráfico de multimedia es bastante pesado lo cual genera que operen en altas tasas de transmisión y de esta manera las huellas de carbono son mas altas.

En las redes de IoT los dispositivos están equipados con diferentes fuentes de energía, por ejemplo, baterías de litio, celdas solares, energía piezoeléctrica, entre otras. Por lo tanto la comunicación verde se puede adoptar mediante la implementación de nodos equipados con una fuente de energía verde que garantice una reducción significativa de las emisiones de carbono (Wade Trappe, 2015).

Estos dispositivos producen gran cantidad de residuos electrónicos y también consumen una cantidad significativa de energía para ejecutar sus diferentes tareas. Este finalmente es el reto que más preocupa a los investigadores y desarrolladores para poder minimizar el consumo de energía. La visión se ha vuelto cada vez mas compleja para las aplicaciones de alta tecnología que necesitan un nivel de consumo mayor, pero como un contexto generalizado el consumo de energía se ha convertido en una cuestión fundamental en el

futuro del internet y de los diferentes enfoques que se desarrollan (Sarder Fakhrul Abedin, 2015).

Por esta razón los nuevos desarrolladores de aplicaciones y dispositivos se encuentran enfocados en dedicar la mayor parte de su energía y computación para la ejecución de la funcionalidad principal de la aplicación y de esta manera poder garantizar la seguridad y privacidad que necesitará también los diferentes dispositivos.

Los avances de las tecnologías inalámbricas, junto con la minimización de los dispositivos, ha dado lugar a un tejido de comunicación bastante importante que abarca prácticamente todo lo de la vida cotidiana del ser humano; desde automóviles, sensores ambientales, comunicación personal, productos sanitarios, etc. Iot incluirá dispositivos de todos los tamaños los cuales algunos pueden utilizar sus recursos adecuadamente y otros necesitarán ser recargados constantemente. Sin embargo, estos dispositivos al ser tan asequibles necesitarán en término de energía un límite, para de esta manera no colapsar el medio ambiente por saturación de energía eléctrica (Wade Trappe, 2015).

Algunos de los principales retos en la investigación de IoT han sido identificados por los investigadores, entre estos retos se encuentren: escalabilidad, heterogeneidad, interoperabilidad y la seguridad. Un estudio reciente demuestra que alrededor de 26 millones de dispositivos estarán conectados en el año 2020 (Saint, 2015).

5.1 Dispositivos físicos

Cuando se habla de dispositivos físicos, se relaciona cualquier tipo de objeto o cosa que se vaya a interconectar en la red de comunicación, con el objetivo de intercambiar

información y garantizar el desempeño de una determinada aplicación, según expertos de la temática los dispositivos físicos tendrán 4 niveles de inteligencia:

- Nivel 1: El objeto será capaz de realizar su identificación de manera única.
- Nivel 2: El objeto podrá saber su ubicación y registros de ubicaciones anteriores.
- Nivel 3: Será capaz de comunicar su estado a un servidor o al nodo de control para actualizar sus características y funcionamiento.
- Nivel 4: el dispositivo será capaz de contextualizar su entorno y de esta manera aprovechar el máximo de sus recursos en pro de desarrollo.

Sin embargo, existe otro nivel en el cual esta prácticamente diseñado para la conectividad entre los objetos, es decir, que cada dispositivo tenga el criterio necesario para satisfacer sus necesidades de interconexión con los demás dispositivos que se encuentran en la red por medio de uno sensores que garantizan el flujo de datos para un procesamiento futuro.

La red de IoT se compone prácticamente de dos sensores, uno para la parte inalámbrica y la otra para los dispositivos físicos. Los dispositivos de sensores tiene la capacidad de contener memoria y procesamiento de datos con una baja potencia; por el contrario algunos dispositivos físicos tienen un mejor procesamiento pero su consumo de potencia es mayor (Shelby, 2010).

Es en este punto donde se empieza a investigar para lograr que los dispositivos físicos se encuentren en un escenario óptimo para un consumo bajo de energía, lo que se plantea para estos dispositivos es que actúen como nodos de retransmisión lo que disminuiría considerablemente su consumo.

Al realizar esta retransmisión a un nodo central en el cual facilitará la comunicación con el servidor web, mejorando considerablemente la conectividad y la capacidad de interactuar con otros dispositivos, garantizando un flujo continuo de datos con menor consumo de potencia y a una velocidad óptima, debido a que todo el procesamiento se realizará en el servidor web (Shelby, 2010).

Los nodos de retransmisión producen los datos y estos son enviados a un nodo central para que cada uno de los nodos puedan redirigir sus datos al servidor web incorporado para su posterior procesamiento.

5.2 Servidor web

El servidor web tendrá la capacidad de explotar la conectividad con cada uno de los dispositivos a través de internet. Los datos y funcionalidades son consideradas como recursos y se pueden acceder directamente a través de los identificadores RFID. Sin embargo, este servidor aumentará su consumo de potencia debido a que todo el procesamiento de los dispositivos físicos se realizará en este punto.

La arquitectura básica de este servidor se compone de cliente-servidor con algunas limitaciones dependiendo del protocolo que se esta manejando. Vale recalcar que las aplicaciones son simples, ligeras y permiten una respuesta bastante eficaz, ideal para entornos en los cuales los recursos sean limitados, como por ejemplo, espacios pequeños como el hogar que se busca reducir el consumo de potencia y que a su vez el tiempo de respuesta sea óptimo (Thibaut Le Guilly, 2013).

La principal tarea de estos servidores será disminuir la brecha que se genera entre los dispositivos físicos y el tamaño de la red, esta comunicación será realizada por el protocolo http que se hará entre los dispositivos físicos y el servidor web. En esta comunicación se establecerá toda la información de los dispositivos, la identificación del producto, la identificación MAC, la asignación de la dirección IP del dispositivo y la notificación adecuada para que el servidor cree un objeto virtual en la nube con cada una de las características obtenidas anteriormente (Thibaut Le Guilly, 2013).

Todas estas tareas realizadas por el servidor web aumentan considerablemente el consumo de potencia, sin embargo, dependiendo de su programación en la red, disminuye el consumo de potencia en los dispositivos físicos. Esto es algo beneficioso para lo que se quiere del ahorro de energía, ya que tiene la capacidad de poner inactivos los dispositivos que reaccionan a bajas peticiones y el consumo de energía será directamente proporcional a la utilización del dispositivo (Thibaut Le Guilly, 2013).

5.3 Entorno de la nube

Cuando se habla en un contexto de la nube se puede definir en tres parámetros:

- Entorno Virtual: Este entorno proporciona el soporte de la virtualización de los objetos o dispositivos físicos en el servido web. Será sede de cada uno de los objetos virtuales que se creen, también tiene la responsabilidad de la seguridad de estos objetos para evitar vulnerabilidades en estos.

  La asignación de los recursos se realiza dependiendo de la solicitud del servicio a la cual el usuario quiera acceder realizando de esta manera un ahorro de energía

considerable ya que solamente se asigna recursos con la petición y no envía constantes mensajes que gastan energía (Srdjan Krco, 2014)

- Servidor de aplicaciones e interfaz: El servidor de aplicaciones tiene la capacidad de comunicarse con el cliente a través de la interfaz con el fin de acceder a la administración para cualquier tipo de modificación necesaria; tiene la capacidad de realizar un seguimiento de los servicios y dispositivos que están actualmente disponibles en la red y por lo tanto realiza un registro de los cuales se encuentran activos en el instante, reduciendo la búsqueda exhaustiva de y esta manera un ahorro de energía (Srdjan Krco, 2014).

  La actividad del entorno virtual y los dispositivos físicos serán objeto obligatorio de seguimiento para el servidor, ya que este notificará cualquier cambio que se presente en la red, optimizando esta de una manera adecuada.

- Aplicación repo: Repo es una aplicación que tiene la finalidad de responder por cada uno de los servicios de búsqueda para los objetos y basado en un resultado anterior, todo almacenado en cache; al realizar esta tarea se ahorran recursos de búsqueda agilizando de esta manera el tiempo de respuesta y el tiempo de actividad de los dispositivos.

Sin embargo para corroborar el funcionamiento de esta aplicación, al momento de su instalación realiza pruebas de pre búsqueda con el fin de garantizar que las futuras peticiones requeridas se encuentren almacenadas en cache y de esta manera optimizar todos los tiempos. Esta aplicación también envía el resultado de cada una de las pruebas para que sean analizadas y de esta manera reutilizar la información más confiable para futuras búsquedas (Srdjan Krco, 2014).

5.4 Microgrid

En la cumbre de energía limpia desarrollada en Las Vegas, Estados Unidos; el instituto de energía de SIEBEL, una organización de concesión de subvenciones y la investigación, estima que $2000 millones de dólares están siendo invertidos con el objetivo de mejorar la infraestructura de energía a nivel mundial. Una de las novedades que se mostró en esa cumbre son las creaciones de micro redes para la modernización de la energía diseñadas para cambiar rápidamente entre una variedad de fuentes de energía, incluyendo energía renovable (Catherine, 2015).

Las micro redes utilizan redes de sensores en los cuales se analiza en tiempo real los sistemas de control y de esta manera tener la capacidad de proporcionar un marco para responder rápidamente a las demandas de energía requeridas, para asegurar el uso mas eficiente de las diferentes fuentes de energía (Catherine, 2015).

Un despliegue que se esta realizando a grandes pasos es el Internet Consorcio Industrial (CII) una organización que junto con National Instruments (NI) y Cisco están creando la comunicación y control del banco de pruebas para aplicaciones de micro redes en la industria y de esta manera empezar su implementación en las diferentes aplicaciones enfocadas hacia IoT. Las innovaciones en tiempo real proporcionan programas de mensajería que se utiliza para conectar una variedad de dispositivos tales como micro controladores o actuadores que controlan los procesos en sistemas distribuidos como micro redes. Una actualización bastante útil en redes M2M (maquina a maquina) (Catherine, 2015)

Green Energy Corporation es uno de los principales clientes de las innovaciones en tiempo real, ya que utiliza una plataforma basada en la nube de código abierto que sirve de interfaz entre una micro red y de la red de suministro eléctrico local, mientras que también la integración de los datos relacionados con el tiempo, precios en la electricidad, es de vital importancia para la gestión y la evolución de esta tecnología (Catherine, 2015).

Imagen 10 Conceptuañización de una microgrid

Fuente: Green Energy Corp. Microgrid Overview

Green Energy Corp, esta apuntando a sus servicios no solo a las ciudades interesadas en desarrollar las micro redes, sino también para entidades militares que con el tiempo han venido adoptando el uso de IoT. El objetivo es procurar que todos los dispositivos tengan la capacidad de soportar la energía que se suministre en diferentes ambientes y teniendo en cuenta que se esta buscando el uso de energía renovable con el objetivo de reducir costos y pensar en un sistema ecológico propicio.

Por esta sencilla razón los usuarios comerciales quieren reducir los costos de energía, como por el consumo de energía generada en el sitio y vender el exceso de energía a los servicios

públicos locales, al tiempo que reduce sus emisiones de carbono, ya sea para cumplir con las metas internas de IoT o como simplemente una manera de inversión (Catherine, 2015).

5.5 Green-RLP

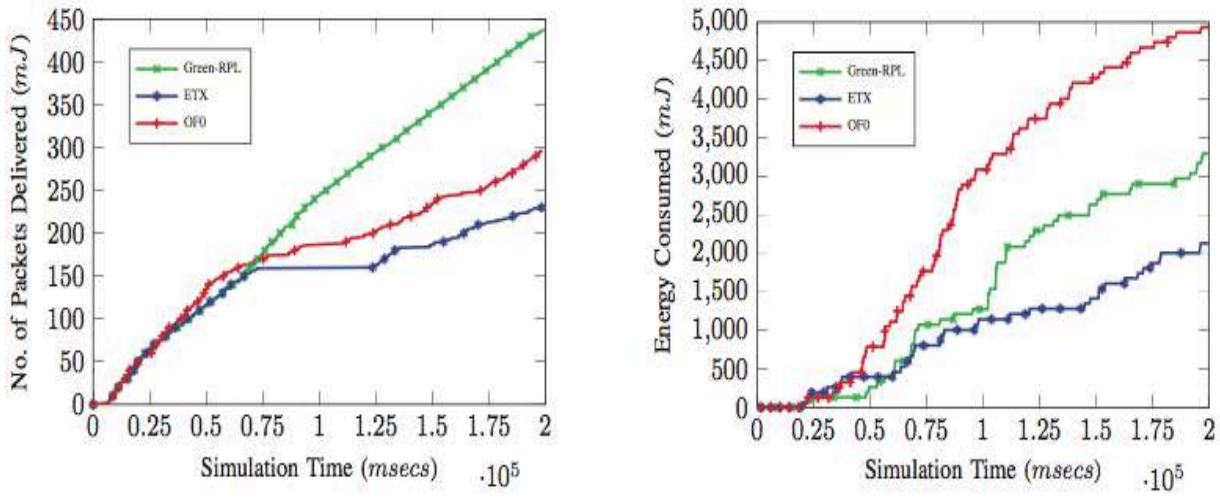
Los dispositivos inteligentes en sistemas de IoT se han desplegado de una manera exponencial, aumentando de esta manera el costo y el tamaño de la red. Además, se supone que estos dispositivos tienen recursos limitados para funcionar en cuanto a potencia, e aquí donde se empieza a desarrollar diferentes aplicaciones y tecnologías para el ahorro en cuanto a potencia de los dispositivos.

En diferentes escenarios típicos de IoT, como el hogar, la industria, la salud, etc., se ha demostrado un aumento de uso de energía, además con ayuda de diferentes protocolos y tipos de enrutamiento de datos a través de un menor consumo de energía, gracias a que evitan que el dispositivo consuma energía en la transmisión y recepción de datos. Sin embargo, los dispositivos de baja potencia al momento de realizar intercambio de datos multimedia los cuales tienen un mayor volumen de información, requieren mayor ancho de banda.

Por lo tanto, la transmisión de paquetes se lleva a cabo con mayor frecuencia y los radios se mantienen a una misma distancia por el tamaño de las redes, lo que se traduce en un mayor consumo de energía y emisiones de carbono mas altos. En consecuencia, el uso eficiente de energía y la operación de comunicación es mas critica para los archivos y datos de multimedia y de esta manera la vida útil de la red disminuirá por el consumo de energía.

En distintos estudios realizados por Green Energy corp demuestran que usando este tipo de energía por medio del protocolo RLP se ven resultados satisfactorios en cuanto a mayor transmisión de datos con un consumo menor de energía, estos datos son comparados con otras dos tecnologías que no se hablarán en este trabajo debido a que su uso en la actualidad es menor a comparación con esta de Green-RLP.

Imagen 11 Comparación de GreenRLP con otras tecnologías



Fuente: Sarder Fakhrul Abedin, A System Model for Energy Efficient Green-IoT Network

En la imagen 11 se ve una clara diferencia, en la primera gráfica con relación al número de paquetes enviados con respecto a un tiempo, en la segunda se observa el gasto en energía consumida con relación a un determinado tiempo. Estos resultados demuestran que utilizar Green RLP tiene un beneficio ecológico ya que necesita menos consumo de energía para que cualquier dispositivo funcione correctamente (Gill, 2013).

Estos resultados demuestran que la aplicación RLP minimiza considerablemente la emisión de la huella de carbono y garantiza el uso adecuado de la energía. Para asegurar la calidad

de servicio suficiente para esta aplicación especifica se preestableció un retardo determinado, por ejemplo, sobre voz IP es de 120ms, mientras que para videos y multimedia puede variar dependiendo de destino del paquete y su tamaño.

6 SEGURIDAD

Las tecnologías y las aplicaciones enfocadas a IoT en el campo de la seguridad aumentan debido a la vulnerabilidad que se puede presentar en la red o en el control de acceso y la presencia de distintos usuarios aumentan el riesgo de que los sistemas en algún momento puedan colapsar (Porkodi, 2014).

Un punto de partida natural para la identificación de los problemas de seguridad de IoT, son las redes inalámbricas y la seguridad en las redes EPC. Esto presenta una mirada hacia el futuro en cuanto a los interesados en la seguridad de los dispositivos inalámbricos, en aspectos como la confidencialidad, la integridad, la autenticidad y la disponibilidad (Wade Trappe, 2015). Pero son tres amenazas las que inquietan a los desarrolladores en la conexiones inalámbricas:

- La confidencialidad: la comunicación inalámbrica entre los dispositivos es especialmente susceptible a las amenazas de confidencialidad de los atacantes. Como los mensajes se transmiten por el aire, los adversarios malintencionados pueden interceptar fácilmente paquetes, por esta razón la comunicación sin cifrar es un riesgo ya que los atacantes pueden decidir que se transmite y que no (Wade Trappe, 2015).
- La integridad y autenticación: Los diferentes dispositivos deben establecer integridad y autenticidad en varios niveles, esto requiere la capacidad de poder autenticar cada uno de los dispositivos en la red y asegurar que la integridad de la comunicación de los mensajes entre los emisores y receptores tengan la confianza de que sus datos entran al sistema sin ningún riesgo (Wade Trappe, 2015).

- Disponibilidad: Los adversarios pueden lanzar ataques con el objetivo de inhabilitar el funcionamiento o denegar la comunicación de modo adecuado entre ellos. Del mismo modo, los ataques podrían implicar una reprogramación de los dispositivos inalámbricos para poder operar de nuevo en su ciclo de trabajo cotidiano, de esta manera afectando la disponibilidad y saturando los servidores de peticiones falsas (Wade Trappe, 2015).

Por estas tres características se empiezan a desarrollar técnicas con el objetivo de mejorar la seguridad y garantizar que la accesibilidad a internet sea confiable. Muchos de estos dispositivos proporcionan información de manera inadecuada, con lo cual es necesario mantener un control constante. Como tal, el IoT asume nociones previas y separadas de las redes de sensores, redes móviles y sistemas RFID, para asegurar que IoT requiera de técnicas que apoyen estas áreas de forma inteligente (Gill, 2013).

6.1 Gestión de identidad

La gestión de identidad (idM) es un componente de la estructura de seguridad que se encarga de gestionar las identidades de un objeto inteligente de una manera privada y fiable. Se basa en el uso de sistemas de credenciales anónimas, que permite a los dispositivos identidades parciales que se utilizarán para una transacción especifica entre la comunicación con otros dispositivos.

Con el fin de lograr la funcionalidad requerida, es necesario seguir unas reglas de privacidad que se utilizan para definir las preferencias de privacidad a los usuarios para una selección adecuada de sus identidades parciales en función de sus condiciones de contexto actual. Estas reglas son evaluadas por un subcomponente selector de identidad, que se

puede utilizar para gestionar los diferentes contextos en los cuales estas identidades parciales tengan que ser usadas (José L. Hernández-Ramos, 2015).

Cabe señalar que las políticas de privacidad de los dispositivos inteligentes que interactúan en la comunicación podrían requerir diferentes atributos para ser establecida, para solucionar esa situación se realiza un proceso de negociación, suponiendo el caso en el cual el servicio de destino requiere atributos más la identidad del solicitante, así que la política será diferente debido a la cantidad de información que esta comunicación conllevará. En este sentido se compara la política de privacidad del dispositivo de destino y se puede establecer la mejor identidad parcial para adoptar (José L. Hernández-Ramos, 2015).

6.2 Seguridad en dispositivos generadores de datos

Los dispositivos serán generalmente de baja potencia con procesamiento limitado y con capacidad de almacenamiento, esto podría inhibir la capacidad del dispositivo para llevar a cabo cualquier cifrado, ya sea en lo que respecta a los datos almacenados como a la información que se transmite por medio de la red (Moffatt, 2015).

Los propios dispositivos también tienen que realizar algún tipo de registro o mapeo, ya sea a un concentrador local o a una aplicación física. Desde una perspectiva de red, tecnologías como infrarrojos y bluetooth, permitiendo al mismo tiempo el acoplamiento sencillo y transferencia de datos, han históricamente brindado oportunidades para el cifrado de clave mise. Otra oportunidad para el compromiso de seguridad podría potencialmente provenir de los dispositivos cuando estos no se encuentren en línea. Uno de las cosas fundamentales de IoT es que los dispositivos siempre van a encontrarse interconectados, esto permite una comunicación bidireccional con uso de recursos (Moffatt, 2015).

Utilizando un algoritmo llamado punto política de decisión sencilla (PEP) los dispositivos pueden llevar acciones permitiendo el acceso o responder una integración entre ellos, si el dispositivo local tiene que comunicar para tomar una decisión este informará si esta en la capacidad garantizar la seguridad para poder transmitir esa información por la red. Todo esto debido a que los dispositivos tienen que capturar y recibir datos, así que la autorización tiene que ser constate (Moffatt, 2015).

Sin embargo la autenticación de dispositivos es fundamental para evitar que ambos dispositivos se puedan comunicar con otro que no cuente con la autorización pertinente y se genere una lectura de datos malicioso, ya que el dispositivo indeseado lo que hará es intentar saturar la red con el objetivo de evitar la disponibilidad y fiabilidad de la red (Moffatt, 2015).

6.3 Privacidad de datos

El cifrado de datos entre los dispositivos interconectados que se encuentran listos para la comunicación es bastante importante, desde un punto de vista de tránsito y almacenamiento es un parámetro a tener en cuenta. Esto en teoría, podría ser un rompecabezas complejo de resolver con el objetivo de procurar que los datos en si requieran un propietario, que alguien sea responsable cuando se trata en la cuestión de tomar decisiones (Moffatt, 2015).

Los datos en si puede también requerir etiquetado, de una manera similar al sistema utilizado por los gobiernos de muchos países, por ejemplo, la forma de numerar los registros civiles de los ciudadanos. Todos estos temas de gestión tienen que ser comprendidos, analizados y observados de una manera aplicada sencilla, de esta manera

poder garantizar la fiabilidad e la información y poder ser aplicada a un mundo de consumo que día a día es más escalable (R. Johnstone, 2008).

6.4 Autorización, autenticación y contexto

Los sistemas de seguridad en IoT requiere varios componentes para su perfecta funcionalidad, La autenticación (Confirmación de la verdad de la identidad) y la Autorización (Confirmando lo que la identidad tiene acceso) son los dos componentes principales. Sin embargo, ambos requieren de un contexto con el fin de mejorar la toma de decisiones y estar totalmente optimizado (Berners-Lee, 2010).

Un claro ejemplo de la autenticación para una identificación puede ser nombre de usuario y contraseña. La autenticación juega un papel importante en el panorama de los datos, ya que contiene toda la información de los propietarios, los generadores de información, entre otras, así que todos tienen que ser verificados e identificados de manera exhaustiva (Moffatt, 2015).

Sin embargo, el anterior ejemplo era para una autenticación de personas, como en esta oportunidad se requiere una autenticación de comunicaciones entre maquina a maquina (M2M), el dispositivo necesita un proceso que permite la prueba de su identidad con el fin de validar los datos que pueden llegar a generar. De esta manera, los datos se cifran con diferentes algoritmos como por ejemplo, Infraestructura de Clave Pública (PKI) o JSON fichas web, que se utilizan para realizar las autenticación de cada uno de los dispositivos interconectados (R. Johnstone, 2008).

Así que en conclusión, los consumidores de datos requieren tanto autenticación como autorización, las cuales permiten la verificación de la identidad y permiten el acceso a determinados aspectos para el consumo de la información.

6.5 Mecanismos y estándares existentes

El internet y el enfoque de la identidad de las cosas contienen muchos componentes que van en constante evolución. Estos componentes incluyen la mecánica para las cosas como el registro de usuarios, propietarios, la autenticación, autorización a través de las comunicaciones y del almacenamiento de cada uno de los dispositivos inteligentes conectados en la red (Thibaut Le Guilly, 2013).

A partir de una red y del almacenamiento de datos se ha convertido un enfoque común para los desarrolladores web que operan en un entorno independiente de la plataforma, donde los teléfonos móviles y sitios web se pueden combinar. Un ejemplo de esto es JSON (RFC 7159) que autentica y OAuth2 (RFC 6749) y OpendID (RFC 6616) que se encargan de proporcionar la autorización. Estos estándares desarrollados tiene un papel importante en la comunicación actual entre los dispositivos debido a la garantía de la comunicación que estos generan (Thibaut Le Guilly, 2013).

OAuth2 es quizás el estándar más popular para los consumidores ya que permite a los clientes de terceros poder acceder a la información no primordial de la red pero que sin embargo sirve para la comunicación con las otras redes, esta información garantiza la confiabilidad de los perfiles y atributos de cada una de las redes vecinas. También permite al titular de los datos eliminar el acceso concedido anteriormente simplemente con una contraseña (Moffatt, 2015).

Sin embargo, lo más preocupante para los desarrolladores son como tantos protocolos, dispositivos y estándares se pueden comunicar de entre ellos, volviendo la información más fácil de obtener para los maliciosos . Por esta razón, se esta manejando infraestructura más robusta en la web, donde cada red tenga la posibilidad de personalizar su acceso y de esta manera mantenerse separados de los demás registros en cuanto no sean solicitados de alguna manera (Amel Achoura, 2015).

Basados en estos estándares de integración las infraestructuras pueden proveer información de los sitios y permitir la identidad de los proveedores con el fin de garantizar el despliegue potencial de la información por medio de las plataformas estructuradas adecuadamente para que esta no corra ningún tipo de riesgo y complete su finalidad (Amel Achoura, 2015).

6.6 Confianza y reputación

La confianza y reputación (T&T) son componentes que permiten establecer un ambiente de confianza fiable donde cada uno de los dispositivos de IoT puedan interactuar con el servicio de la red de una manera segura. Estos componentes reúnen información continuamente desde el administrador para poder cuantificar la confianza de forma adaptativa.

Estos componentes pueden depender de diferente información de contexto, por ejemplo, información de seguridad, de esta manera la confianza y reputación empezarán su proceso para garantizar la seguridad de ellos. Un punto a favor de esta recolección de información adaptativa es que se basa en evidencias históricas los cuales se pueden clasificar para encontrar patrones en donde se garantice la seguridad en aspectos que fueron vulnerables anteriormente (R. Johnstone, 2008).

Todo esto conlleva a que los dispositivos inteligentes puedan obtener información y datos de otras redes de una manera fiable, asegurando que los datos obtenidos solo provienen de los objetos inteligentes que satisfagan ciertos puntajes de confianza, en los cuales las puntuaciones se pueden utilizar como credenciales con el fin de tomar decisión de control de acceso más confiable (Thibaut Le Guilly, 2013).

Todo esto se puede garantizar gracias al uso de algoritmos y técnicas que calculan la fiabilidad de una determinada entidad, así que computacionalmente debe tenerse en cuenta algunas restricciones como lo son el consumo de energía y el almacenamiento, lo que genera una reputación agradable a cada una de las redes. Basado en los diferentes resultados que se obtienen el servidor madre de cada red puede interactuar con sus clientes y de esta manera optimizar la cantidad de recursos que se disponen en la red (Thibaut Le Guilly, 2013).

7 CAMPOS DE APLICACIÓN DE IOT

Las ciudades inteligentes se convierten en un nuevo paradigma en la era de la información y la tecnología de la comunicaciones (TIC), que proporciona la infraestructura para que los ciudadanos tengan acceso a muchos servicios fácilmente, y para los órganos de gestión y control de los recursos en una ciudad inteligente sean distribuidos de una manera adecuada. Las ciudades inteligentes utilizan las TIC para detectar, analizar e integrar la información para que las ciudades y personas funcionen de una mejor manera (Aditya Gaura, 2015).

A medida que las poblaciones de las ciudades van creciendo y los limites en cuanto expansión territorial disminuyendo, el concepto de ciudad inteligente gana impulso para transformar las ciudades y mejorar de alguna manera la calidad de vida, el crecimiento económico, el progreso tecnológico, el progreso del medio ambiente y la sostenibilidad autónoma de cada ciudad (Aditya Gaura, 2015).

La evolución de la tecnología se ve reflejada en varios aspectos, uno de ellos es la comunicación móvil que se ha expandido en los últimos años, hoy en día hay más de 5,6 millones de teléfonos móviles en uso en el mundo. Cada llamada, texto y mensaje instantáneo contribuye a la gran cantidad de datos generados cada día. Los dispositivos móviles especialmente los inteligentes y las tabletas, tienen varios sensores incorporados con tantas aplicaciones que se pueden usar con el objetivo de compartir datos recogidos por cada uno de estos sensores (Aditya Gaura, 2015).

Sobre la base de la expansión y el desarrollo de la tecnología, los datos se han incrementado en la escala de múltiples campos, entre los cuales sobresalen: transporte, salud, hogar, industria y la seguridad pública, dentro de estas áreas existen bastantes

aplicaciones bastante útiles para el ser humano, entre las que se encuentran: la domótica, telemedicina, automatización en la industria, etc. (Dr. Peter Friess, 2012).

Para Colombia el término de IoT resulta bastante atractivo por la variedad de aplicaciones que se pueden desarrollar, en áreas como el transporte, la salud, el hogar, la seguridad pública y el deporte, abriendo de esta manera una infinidad de posibilidades de investigación en la facultad de ingeniería de telecomunicaciones de la Universidad Santo Tomás.

7.1 Transporte

En los últimos años, muchos vehículos como trenes, automóviles, bicicleta, aviones y barcos se están equipando con sensores. Estos tipos de sensores pueden recoger algo de información sobre la ubicación, velocidad y estado de los objetos. Al contar con esta información se puede gestionar el tráfico, las rutas y la contaminación del aire en las ciudades.

También equipando paquetes e información se puede rastrear todo con etiquetas RFID de tal manera que el control del estado del medio de transporte y de lo que se transporta puede ser gestionado en distintos puntos geográficos. Un claro ejemplo de todo esto, son la gran variedad de aplicaciones tales como la conducción asistida, venta de entradas móvil, vigilancia y mapas de GPS asistida, que en la actualidad cogen un peso importante en el diario vivir.

La ciudad de Bogotá es un ambiente en el cual el transporte juega un papel importante entre sus habitantes, a tal punto que crea múltiples oportunidades de implementación de IoT. Es

por ello que se pueden generar oportunidades de investigación dentro del grupo INVTEL, alguna posibles ideas son:

PLAN A IMPLEMENTAR	RECOMENDACIONES
Control de rutas del transmilenio: Por medio de sensores dentro de cada vehículo articulado, donde se lleve un control de tiempo entre cada uno de ellos, con un registro que cuente el tiempo exacto a su próxima parada teniendo en cuenta factores como: estado de las vías, semáforos y posibles congestionamientos y de esta manera brindar diferentes soluciones a los usuarios. Sin embargo, es necesario sensores de movilidad dentro de las estaciones para determinar posibles demoras en cada parada de los vehículos.	• Para una aplicación de este estilo es recomendable utilizar un protocolo RLP, ya que brinda la posibilidad de transmitir durante el desvanecimiento de la señal inalámbrica (EL vehículo se aleja de la estación), ya que cuenta con una memoria temporal que puede ser descargada en la próxima estación proporcionando toda la información requerida. • Para ahorrar energía se puede implementarla tecnología Green-RLP, ya que los radios de transmisión serán cortos y de esta manera se puede transmitir paquetes a mayor frecuencia, reduciendo considerablemente el uso de energía, ya que la operación de comunicación

	solo se realizará en un rango cercano a las estaciones. • La seguridad de esta información es simplemente de gestión, autorización y autenticación, debido a que solo se manejarán datos estadísticos que permitan realizar un algoritmo de calculo y de esta manera determinar con exactitud el tiempo de llegada.
Sensores entre vehículos que organicen un plan de evacuación para las ambulancias. Las ambulancias se convierten en prioridad en las vías de cualquier parte del mundo, si se realiza una red vehicular donde informe por cual carril viene la ambulancia y de esta manera por medio de un plan realizado por una aplicación informe a cada conductor su posible movimiento y de esta manera la ambulancia cuente con una velocidad constante para resolver su emergencia.	• Un protocolo MIPv6 seria el adecuado para resolver esta aplicación en una red MANET, ya que se realizará redes dependiendo del sector de la ciudad donde se encuentre, asignando direcciones IP a cada vehículo y de esta manera llevara un control del estado de su red e informar la ubicación exacta para predecir los movimientos adecuados de cada coche. • Para el control de energía es propicio utilizar microgrid ya que analiza en

	tiempo real los sistemas de control y de esta manera tiene la capacidad para proporcionar la energía requerida cuando este bajo demanda el sensor y de esta manera se garantiza un dispositivo en semireposo pero en constante comunicación. • La seguridad juega un papel importante en este tipo de redes, es necesario utilizar una seguridad en los dispositivos generadores de datos ya que como van a trabajar con baja potencia un capacidad de cifrado es menor, por tal motivo es necesario utilizar PEP que permite el acceso e integración entre los dispositivos de la red con un cifrado único y seguro.

Tabla 1 Posibles soluciones transporte público de Bototá

Con estas soluciones se puede garantizar una mejora en diferentes aspectos de la rutina del transporte de la ciudad de Bogotá, la primera aplicación es bastante similar a la predicción del tiempo que se tiene actualmente en las estaciones, sin embargo, esta actualización

mejora considerablemente los tiempos ya que utiliza otros aspectos y factores que se controlan por medio de redes que pronostican la calidad del servicio. Y la segunda aplicación garantiza un menor tiempo de transito entre el lugar de donde se encuentra el paciente y cualquier entidad hospitalaria, aumentando las posibilidades de vida de algunos pacientes.

7.2 Seguridad pública

Las ciudades con poblaciones mayores a menudo tienen mayores tasas de delincuencia. Sin embargo, las ciudades grandes también sufren de mala educación y altas tasas de desempleo que crean un cultivo para la actividad delictiva. En los últimos años el registro de delincuencia a nivel mundial se lleva a cabo con métodos tecnológicos que han mejorado la eficiencia de los productos (Roozbeh Jalali, 2015).

Estos datos no solo tiene un registro detallado del crimen sino que también proporcionan un patrón de modus operando de los delincuentes generando así una mejora en las investigaciones realizadas. Durante muchos años los criminólogos y estadísticos han estado utilizando habilidades y conocimientos para predecir el tiempo y el lugar de la aparición de la siguiente serie de crímenes con diferentes grados de éxito (Roozbeh Jalali, 2015).

A partir del 11 de septiembre el uso de la minería de datos se ha aumentado considerablemente en diferentes áreas como la detección de delitos y perfiles de comportamiento. Estos perfiles busca patrones de comportamiento utilizando la información digital disponible encontrado en diversas base de datos y reconoce las actividades delictivas con el fin de encontrar culpables (Roozbeh Jalali, 2015).

La minería de datos, al igual que con el análisis criminal, tiene el mismo objetivo general : la detección y prevención de delitos. Con una plataforma de ciudad inteligente que le instale cámaras y sensores alrededor de la ciudad para monitorear automáticamente cada una de las actividades delictivas. También hay potencial para predecir crimines basados en la actividad de los ciudadano en las redes sociales (Roozbeh Jalali, 2015).

La seguridad de la ciudad de Bogotá es un reto para cualquier gobierno, debido a su expansión territorial y la gran cantidad de habitantes que posee, pero con la implementación de IoT se puede generar aplicaciones que garanticen y mejoren la seguridad de las calles de la siguiente manera:

PLAN A DESARROLLAR	RECOMENDACIONES
Realizar una implementación de cámaras sectorizadas que garanticen una visualización clara de los rostros de los transeúntes, para que de esta manera por medio de sensores de movimiento y reconocimiento de rostros se pueda predecir diferentes patrones establecidos que puedan garantizar los posibles delitos a cometer y de esta manera realizar el seguimiento pertinente a los delincuentes.	• Por la complejidad de la información que se transmitirá en este tipo de red, es necesario usar SDN, ya que garantiza un aumento considerable en la funcionalidad de la red, reduciendo costos y aumentando la complejidad del hardware que se tenga implementado. • La energía puede ser controlada por los mismos dispositivos físicos que

	garanticen un mejor procesamiento a bajo consumo de energía, dependiendo del estado de las calles y el movimiento que se este presentando en ellas. • La seguridad se tiene que implementar con varios sistemas de control que garanticen un funcionamiento constante, y al mismo tiempo tenga la capacidad de controlar la autorización y autenticación de los registros de la base de datos para encontrar los parámetros y predecir los posibles delitos a cometer.

Tabla 2 Posible solución a la seguridad pública

7.3 Salud

Existe un rápido progreso en el desarrollo de la asistencia sanitaria inteligente y vigilancia de la salud en entorno no clínicos de todo el mundo. Tecnología portátil es una de las tecnologías prometedoras que pueden ayudar a monitorear la salud de una forma remota e

inteligente. Debido a la capacidad de disminuir de tamaño y la calidad de los sensores portátiles precisos de hoy en día (Alexandre Santosa, 2014).

Los datos recogidos por los sensores son importante, ya que se pueden procesar con el objetivo de garantizar la mayor cantidad de información que indique la situación actual del paciente, como lo son signos vitales y evolución del mismo, la pregunta que se realizan los usuarios y los expertos en salud es, si trabaja con los datos integrados en las bases clínicas, para de esta manera poder beneficiar al usuario y a la comunidad de una mejor manera (Alexandre Santosa, 2014).

En el hogar los sistemas de monitoreo de sensores y la tecnología constituyen un componente fundamental en una ciudad inteligente. Los pacientes son cada vez más activos en el cuidado de su vida cotidiana y la mejora de sus problemas de salud. De acuerdo con estadísticas del censo de Estados Unidos en 2009, la atención de salud gasto $2,486 billones de dólares, a comparación de una atención medica en el hogar que simplemente gasta $68 Billones de dólares (Expenditures, 2012).

La importancia de la tecnología enfocada a la salud humana se ha especulado para abordar el manejo del estrés y prevenirlo, ya que para muchos pacientes es una tarea complicada dirigirse a los centros de salud y esperar infinidad de tiempo para poder ser atendidos. La privacidad de los ciudadanos es una de las cuestiones más importantes cuando las ciudades se vuelven inteligentes, los autores has presentado modelos básicos de esta vida y la privacidad en todos los aspectos es algo que preocupa a los clientes (H, 2015).

En la 18ª conferencia internacional sobre la inteligencia en redes de próxima generación del 2015, la atención a las caídas, supervisión de las enfermedades crónicas y tele vigilancia de

la fisiología en lugares rurales fue la sensación, ya que utilizando tecnología basada en sensores inteligentes se puede mejorar la vida en aspectos claves de los planes de investigación propuestos para el futuro (H, 2015).

La contaminación es un factor a tener en cuenta a nivel mundial, por lo tanto en una ciudad como Bogotá de constante evolución es importante tener un control y adecuado de los índices de monóxido de carbono para aplicar multas a los posibles infractores de la siguiente manera:

PLAN A DESARROLLAR	RECOMENDACIONES
Sensores de contaminación sectorizados controlados con cámaras de seguridad para multar a los infractores del medio ambiente. Al mismo tiempo aplicaciones móviles para mejorar la ruta sana en la ciudad, es decir, que las personas por medio de una aplicación se conecten con los sensores de contaminación y de esta manera establezcan una ruta por la cual los índices de monóxido de carbono son menores.	• Todo lo relacionado con redes de salud se implementa con redes SDN, por proveer complejidad en el hardware y el constante funcionamiento de la red, ya que se necesita 24 horas de control en un aspecto de este tipo de aplicaciones. • El consumo de energía de cada dispositivo se puede realizar de dos maneras conjuntas, la primera es enviando datos a un determinado tiempo garantizando de esta manera un estado pasivo de los servidores y

	la otra forma son que los dispositivos manejen una microgrid que garantiza el consumo de energía dependiendo del nivel de procesamiento. • Con respecto a la seguridad simplemente es necesario la seguridad de los dispositivos generadores de datos para mejorar y controlar los diferentes contextos en los cuales se maneje la información.

Tabla 3 Solución para la contaminación de Bogotá

La anterior es una idea que puede mejorar la salud de muchas personas, ya que el gobierno puede garantizar multas a los que superen cierto limite de emisión de monóxido y las personas pueden tener el control de sus rutas para intentar respirar un aire limpio y seguro para su cuerpo.

7.4 Hogar

Con la innovación de IoT en diferentes áreas de conocimiento, recientemente se ha empezado a ver signos positivos que indican que el mercado de casas inteligentes será la sensación en muchos aspectos. La idea de una casa inteligente surgió en el año 1923, cuando el arquitecto suizo Le Corbusier describió una casa como una maquina parra vivir.

Desde entonces, se ha visto muchos intento para transformar esta visión en realidad (OLEG LOGVINOV, 2015).

El nuevo enfoque de IoT de transformación de los sistemas inteligentes ha permitido que sea un motor de crecimiento de la próxima generación que esta afectando el ecosistema global de las industrias nacionales e internacionales y la transformación de la vida de las personas en cuanto a su cultura (OLEG LOGVINOV, 2015).

Un número de compañías están lanzando aplicaciones con el mismo enfoque para poder controlar los sistemas de rociadores que riegan el césped, estos sistemas recogen información local de la temperatura y de la humedad para así realizar pronosticaciones del tiempo y determinar la cantidad de agua que requiere el césped para mantenerse en perfectas condiciones (OLEG LOGVINOV, 2015).

Cada uno de los dispositivos inteligentes y sistemas que se están diseñando para ser implementados en el hogar buscan hacer más cómoda la vida del ser humano, mejorando la eficiencia con la que se utiliza la energía, el agua y otros recursos naturales que se encuentran escasos en la actualidad (OLEG LOGVINOV, 2015).

En el hogar son múltiples las aplicaciones que se pueden realizar por tal motivo nombrarlas seria complejo, por tal motivo solo se indicará que el protocolo propicio para estas redes son las MIPv6 ya que permiten una movilidad entre redes, dentro de la casa subredes, garantizando una conectividad máxima entre cualquier punto del hogar.

7.5 Deporte

La finalidad de IoT es implantar tecnología y comunicación en cada uno de los dispositivos que rodean a las personas, por tal motivo con la implantación de esta tecnología en el deporte, comienza a nacer el término de “deporte inteligente”. Este deporte prácticamente será todas las cosas que se encuentren relacionadas con el ámbito de la actividad deportiva.

Hoy en día la tecnología ha alcanzado un punto bastante alto y la mayoría de personas alrededor del mundo han adoptado en sus vidas cotidianas mucha tecnología. Los avances futuros podrían incluir auriculares y relojes, con el objetivo de medir los signos vitales mientras se realiza alguna actividad física, arrojando también resultados de la actividad realizada.

Pero la tecnología de hoy en día es bastante convincente, por ejemplo, unos zapatos inteligentes para jugar baloncesto que utiliza sensores integrados para rastrear a un jugador y de esta manera proporcionar información en tiempo real para una aplicación móvil en donde exponga datos del jugador, como ejemplo, distancia recorrida, fuerza en el salto, distancia de frenado, entre otras.

El anterior es un claro ejemplo de cómo IoT puede ser aplicado en los deportes mejorando numéricamente las aptitudes físicas y buscar posibles mejoras en los atletas dependiendo de sus anteriores registros. Es por esta razón que el grupo de investigación INVTEL, puede mejorar las expectativas de desarrollo en cuanto al área de deporte ya que brinda la posibilidad de investigación en el deporte, tema de poco interés en Colombia.

8 CONCLUSIONES

- El término de IoT resulta complejo porque se puede desarrollar a través de la convergencia de varios desarrollos que interactúan entre si para hacer de IoT una realidad. Es por ello que IoT resulta una de los avances tecnológicos más relevantes de los últimos tiempos, por su desarrollo e investigación.
- La información que circula en la sociedad relacionado con el Internet de las Cosas (IoT), es bastante densa, permitiendo un desarrollo generalizado de cada uno de los parámetros a investigar y querer documentar. Sin embargo, en el ámbito de protocolos no se ve una clara documentación por lo que es necesario acudir a los RFC (Request For Comments)
- Las áreas de investigación que mas tienen valor en el Internet de las Cosas son los protocolos, seguridad y energía, ya que son los parámetros que mas implican desarrollo frente a esta tecnología.
- Frente a los campos de investigación, se puede encontrar infinidad de áreas, sin embargo, es el hogar, la salud, el transporte, la seguridad pública y el deporte los campos en los cuales sobresale esta temática.
- La mayoría de los avances tecnológicos necesarios para el desarrollo de IoT se han desarrollado de forma satisfactoria, de tal manera que algunos fabricantes y entidades ya han empezado a implementar una pequeña escala de lo que conlleva IoT.
- El Iot resulta un mercado a tractivo para cualquier tipo de negocio, sin embargo, requiere de mucha preparación debido a las innovaciones tecnológicas que se denotan día a día.

- Los protocolos desarrollados han permitido que se pueda controlar de manera adecuada la cantidad de datos que circulan a cada segundo por la red, permitiendo una convergencia adecuada de diferentes tecnologías.
- Las diferentes maneras de aprovechar la energía permite un desarrollo investigativo bastante alto, hasta el punto de lograr por medio de programación el menor consumo de energía posible, reduciendo considerablemente el impacto ambiental.
- El consumo de energía es uno de los factores que más preocupan en el desarrollo de cualquier aplicación debido a la conciencia ambiental que esta generando cualquier tipo de desarrollo. Por ello, la necesidad de utilizar energía renovable aumenta las posibilidades de avance a nivel mundial, dejando abierta una temática de bastante interés para la sociedad y la ciencia.
- EL transporte es el área en la cual se tendría bastante desarrollo en Colombia, debido a la complejidad de las carreteras y de las vías del país. El progreso que se tiene en esta área en Colombia es prácticamente nulo, ampliando de esta manera su campo de investigación y desarrollo.
- La salud es sin lugar a duda una oportunidad de desarrollo considerable en un país con zonas altamente rural, debido a la dificultad de acceso a estos lugares se crea la posibilidad de integrar la salud por medio de una automatización del entorno en la cual se ejecute.
- Desafortunadamente el área del hogar en IoT ya se encuentra muy explotada ya que empresas de gran reconocimiento a nivel mundial han puesto varios años de desarrollo e investigación para la mejora esta, por tal motivo no es buen área para la investigación en el grupo INVTEL.

9 BIBLIOGRAFÍA

CÉSAR ANDRÉS GAVIRIA CUEVAS, J. L. (2014). ESTUDIO COMPARATIVO DEL INTERNET DE LAS COSAS FRENTE A LOS PROTOCOLOS TRADICIONALES DE LA DOMÓTICA Y PROPUESTA DE UN PROTOCOLO UNIFICADO. *Universidad Santo Tomas* .

Saint, A. (2015). Where next for the Internet of Things? *ISSA Senior Member* .

Porkodi, D. V.-D. (2014). The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview. *IEEE* .

Shorter, J. S.-S. (2014). Concepts of Identity within the Internet of Things. *IEEE* .

Ren Duan, X. C. (2011). A QoS Architecture for IOT. *IEEE* .

Spring, A. P. (215). Creating Substance from a Cloud: Low-Cost Product Generation. *IEEE*

Jayavardhana Gubbi a, R. B. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *IEEE* .

Heng Li, H. C. (2011). Study on the influence of IoY (Internet of things) on mobile network. *IEEE* .

Stefan Nastic, S. S.-H.-L. (2014). Provisioning Software-defined IoT Cloud Systems. *IEEE*

Gill, H. (2013). *Internet de las cosas- Máquinas, empresas, personas, todo*. From ITU NEWS: https://itunews.itu.int/Es/4503-Internet-de-las-cosas-Maquinas-empresas-personas-todo.note.aspx

Jayavardhana Gubbi, R. B. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions . *SciencieDirect* .

Dr. Peter Friess, D. G. (2012). Europe's IoT Strategic Research Agenda 2012 . *IEEE* .

J. Domingue, A. G. (2013). The Future Internet, Springer-Verlag, Berlin, Heidelberg. *IEEE*

R. Johnstone, D. C. (2008). Smart environmental measurement & analysis technologies (SEMAT): wireless sensor networks in the marine environment, . *IEEE* .

Wade Trappe, R. H. (2015). Low-Energy Security: Limits and Opportunities in the Internet of Things . *IEEE* .

Sarder Fakhrul Abedin, M. G. (2015). A System Model for Energy Efficient Green-IoT Network . *IEEE* .

Shelby, Z. (2010). Embedded Web Service . *IEEE* .

Thibaut Le Guilly, P. O. (2013). HomePort:Midleware for Heterogeneous Home Automation Networks . *IEEE Pervasive Computing and Communications Workshops* .

Srdjan Krco, B. P. (2014). Designing IoT Architecture(s):A European Perspective . *IEEE* .

Sheeraz A. Alvi, G. A. (2015). Energy Efficient Green Routing Protocol for Internet of Multimedia Things . *IEEE* .

Berners-Lee, T. (2010). HyperText Transfer Protocol. *Consurtium* .

Amel Achoura, L. D. (2015). Mobility Management for Wireless Sensor Networks A State-of-the-Art . *ScienceDirect* .

Catherine, M. (2015). Energy and Data Converge in Microgrids. *IoT connect to the internet of things Journal* .

José L. Hernández-Ramos, J. B. (2015). Managing Context Information for Adaptive Security in IoT environments . *IEEE* .

Moffatt, S. (2015). The Identity of Things: Privacy and Security Concerns . *ISSA Journal* .

Roozbeh Jalali, K. E.-k. (2015). Smart City Architecture for Community Level Services Through the Internet of Things . *IEEE* .

Aditya Gaura, B. S. (2015). Smart City Architecture and its Applications based on IoT . *SciencieDirect* .

Alexandre Santosa, J. M. (2014). Internet of Things and Smart Objects for M-Health Monitoring and Control . *SciencieDIrect* .

Expenditures, N. H. (2012). Statistical Abstract of the United States .

H, B. M. (2015). Data mining for wearable sensors in health monitoring systems: a review of recent trends and challenges .

FLAUZAC Olivier, G. C. (2015). New Security Architecture for IoT Network . *SciencieDirect* .

OLEG LOGVINOV, C. (2015). The IoT at Home: Smart Houses, Happy Homeowners. *IEEE* .

MCpro MuyComputer. (n.d.). From Intel IoT unifica la conectividad y seguridad para la Internet de las Cosas: http://muycomputerpro.com/movilidad-profesional/2014/12/10/intel-iot/

Future Markets. (n.d.). From 2DMATERIALS MAG : http://www.2dmaterialsmag.com/new-university-of-manchester-start-up-to-develop-graphene-conductive-inks/

Oracle. (n.d.). From Formatos de direcciones IPv6 que no son los básicos: http://docs.oracle.com/cd/E24842_01/html/820-2981/ipv6-ref-77.html

Microsoft. (n.d.). From Protocolo de mensajes de control de Internet para IPv6 (ICMPv6): https://msdn.microsoft.com/es-es/library/cc757063(v=ws.10).aspx

Ferguson. (n.d.). From Data Service Options for Wideband Spread Spectrum Systems: Radio Link Protocol: http://www.ferguson-by-bicycle.com/sem_lit/is707-2m.htm

McFree. (n.d.). From El protocolo HTTP: http://www.mclibre.org/consultar/php/lecciones/php_http.html

Wikipedia. (n.d.). From Proxy Mobile IPv6: https://en.wikipedia.org/wiki/Proxy_Mobile_IPv6

McPro. (n.d.). From El futuro del Networking pasa por las Software Defined Networks (SDN): http://www.muycomputerpro.com/2013/02/05/pedro-martinez-hp-habla-redes-sdn

GreenEnergy Corp. (n.d.). From Microgrid Overview: http://www.greenenergycorp.com/about-us/about-us/technology/