IV Workshop de Creatividad e Innovación en Informática (IV W - INF)
Internet of Things (IoT) y wearables technologies

Frameworks de Internet de las Cosas y Ciudades Inteligentes basadas Telecomunicaciones y Seguridad

Sergio Gramajo; Reinaldo Scappini; Diego Bolatti; Ricardo Calcagno
Universidad Tecnológica Nacional - FRRe, Argentina
{sergio, rscappini, dbolatti, rcalcagno}@frre.utn.edu.ar

Tema (IA, IoT, smartcities)

Resumen

El crecimiento exponencial de la población y la urbanización sumado al desarrollo de la tecnología y las comunicaciones ha planteado nuevas formas de generar aplicaciones en pos de mejorar los servicios en las ciudades con un impacto directo en la calidad de vida de las personas y el medio ambiente. En este escenario han surgido campos de investigación relacionados a Internet de las Cosas (IoT), ciudades inteligentes, seguridad y la gestión de las telecomunicaciones que interconectan múltiples dispositivos conectados de forma inteligente y con una interacción humana mínima. Debido a este fenómeno, las investigaciones actuales y los organismos de estandarización con las empresas especializadas han propuesto diferentes maneras de generar aplicaciones para ciudades inteligentes e IoT. Sin embargo, las arquitecturas necesarias, la cultura, los estudios de factibilidad técnico-económicos, el uso de las TICs, los aspectos climáticos, las normativas locales o nacionales de uso de telecomunicaciones y espectro, la situación política, entre otros aspectos relevantes, son importantes para proponer soluciones factibles para una ciudad o región. Por lo tanto, en este trabajo de investigación nos vamos a centrar en el análisis de los estándares e investigaciones para que puedan ser transferidos a la región donde se encuentra ubicada nuestra Facultad Regional y proponer soluciones en telecomunicaciones, seguridad e inteligencia.

Palabras clave: IoT; smartcities; seguridad informática

Proyecto que se reporta

Análisis y Aplicaciones de Internet de las Cosas y Ciudades Inteligentes basadas Telecomunicaciones y Seguridad. Código. CCUTIRE5353TC. Centro de Investigación Aplicada en TIC. Universidad Tecnológica Nacional Facultad Regional Resistencia. Director: Dr. Ing. Sergio Gramajo. Investigadores: Mg. Ing. Reinaldo Scappini; Mg. Ing. Diego Bolatti; Ing. Ricardo Calcagno y becarios alumnos. Período 01/2019 – 12/2021.

Este proyecto es una continuidad del proyecto "Modelo para la evaluación de performance mediante identificación de tráfico y atributos críticos en Redes Definidas por Software" - UTN-2422. Además, hay subproyectos asociados a él: 1) Universidades Argentinas en la Unión Internacional de Telecomunicaciones (ITU) y 2) The Use of Computational Techniques to Improve Compliance to Reminders within Smarts Environments (REMIND). Este último en curso de la línea Horizonte2020 de la Unión Europea en el cuál somos partner y participan 7 países de Europa.

Introducción, Justificación

El crecimiento exponencial de la población y la urbanización han intensificado las formas innovadoras de manejar este fenómeno con tecnología y un impacto mínimo en el medio ambiente, los estilos de vida de los ciudadanos y la gobernanza. La integración inicial de las Tecnologías de Información y de Comunicación (TICs) en las ciudades ha promovido los conceptos de ciudad de la información, ciudad digital e Internet de las Cosas (IoT) que apoyan la toma de decisiones en las operaciones de la ciudad de forma inteligente y con una interacción humana mínima [1].

La ciudad inteligente surgió como una solución para abordar los desafíos que surgen con el crecimiento exponencial de la urbanización y la población. Sin embargo, el concepto de ciudad inteligente todavía está evolucionando y no se ha incorporado en todo el mundo debido a barreras tecnológicas, económicas y gubernamentales [1] [2].

Como concepto macro, y en un sentido más amplio, Internet of Things (IoT) fue el resultado de la evolución de las redes convencionales que conectan millones de dispositivos, los avances tecnológicos, las redes inalámbricas de sensores (WSN) y las interacciones máquina a máquina (M2M) [3] [4] con mínima intervención humana es el principio de facto de IoT [5]. Además, los dispositivos conectados entre sí comparten información y tienen acceso a información autorizada de otros dispositivos para luego tomar de decisiones contextuales sobre determinada situación o problema [6].

Como objetivo general se persigue desarrollar modelos de Internet de las Cosas y Ciudades Inteligentes en base a estudios e identificación de atributos sobre telecomunicaciones, seguridad y tecnología que puedan aplicarse a la región.

Objetivos específicos

1. Analizar las arquitecturas y protocolos usados en IoT y Ciudades Inteligentes.
2. Analizar las técnicas de seguridad para los modelos estudiados
3. Desarrollar escenarios de prueba y generación de aplicaciones.
4. Generar posibles transferencias al medio local y/o proponer modelos de estudio para nuestras investigaciones.
5. Desarrollar prototipos de IoT en base a estándares y adaptarlos al medio regional.

Otro de los resultados del proyecto de investigación es lograr un programa de transferencia a empresas del medio y organismos del estado mediante convenios de transferencia tecnológica como el proyecto de estaciones meteorológicas en nodos de fibra óptica para IoT que se encuentra en marcha.

Metodología

Este proyecto incluye el estudio de diversos aspectos tecnológicos y de estándares sobre la infraestructura de redes y de seguridad para la creación de aplicaciones de IoT. Para ello se crearán propuestas sobre escenarios de pruebas o simulaciones con las aplicaciones necesarias.

La metodología será la siguiente:

a) Revisión y análisis de arquitecturas, estándares y protocolos de redes para IoT y Ciudades Inteligentes. Revisión y análisis de esquemas de seguridad para estos sistemas.

Nuestro equipo de trabajo se centrará en estudiar y analizar estas tecnologías y herramientas haciendo hincapié en aspectos de la infraestructura necesaria para nuestra región. Tanto los investigadores expertos en redes, como demás integrantes del equipo participarán de esta actividad.

b) Desarrollo de los escenarios de pruebas para las aplicaciones necesarias. Esta actividad incluye crear los escenarios de prueba para los dispositivos de IoT como microcontroladores y programación de los mismos. En este sentido, nuestro equipo de trabajo seleccionará la tecnología de programación y diseñará el escenario de prueba para las aplicaciones. Ya que el objetivo de este proyecto se orienta al desarrollo de aplicaciones de IoT y Ciudades Inteligentes en nuestra región se podrán usar escenarios simulados como reales según sea el caso. En ellos se validarán los resultados y se podrán contrastar con los resultados esperados y en consecuencia se podrán readaptar los escenarios en caso de ser necesario.

Para estos temas de estudio, el relevamiento bibliográfico se hará en base a diferentes fuentes de información como bases de datos académicas, revistas de producción científica, información de productos de software de tecnología libre o comercial y software para el análisis de seguridad de los datos, consultas a proyectos de investigación relacionados, análisis y solicitud de adquisición de licencias académicas de investigación cuando sea necesario, convenios con proveedores de dispositivos de IoT para fines académicos, etc.

El método de estudio científico a seguir es el siguiente: formulación de hipótesis, en nuestro caso implica el diseño y creación de los escenarios de pruebas simulados o reales en base a estándares o casos de éxitos publicados y publicaciones científicas, lo que incluye aspectos de seguridad determinados y los servicios que se pueden prestar; recopilación de observaciones, en nuestro caso supone llevar a cabo las pruebas de simulaciones o aplicaciones y los escenarios reales identificando atributos factibles en nuestra región; contraste de hipótesis con las observaciones, es decir, evaluar la calidad de nuestras aplicaciones o modelos propuestos y los resultados obtenidos; finalmente, readaptación de las hipótesis iniciales a la luz de los resultados obtenidos, o sea, modificación y refinamiento de nuestros escenarios, ajuste de problemas encontrados en base a la experiencia acumulada..

Desarrollo

Hoy en día existen numerosas aplicaciones de IoT como ser hogar inteligente, ciudad inteligente, almacén inteligente, salud inteligente, sistemas de seguridad urbana inteligente, etc. [7]. Las ciudades que han optado por realizar operaciones o sistemas con IoT y con la ayuda de las TIC se han ido transformando en ciudades más eficientes en varios aspectos como servicios al ciudadano, seguridad, logística, planificación de crecimiento, eficiencia energética, etc. Sin embargo, incorporar las TIC para realizar operaciones en la ciudad no interpreta completamente una ciudad inteligente [8]. La ciudad inteligente es una aplicación del IoT, por lo que hereda el funcionamiento subyacente como se puede observar en la Fig. 1, que implica la generación de datos, la gestión de datos y la gestión de aplicaciones para los ciudadanos.

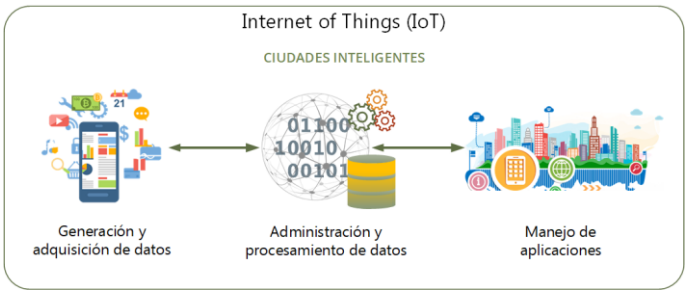

Fig. 1. La contribución de IoT en Ciudades Inteligentes.

Como base de nuestra investigación, en los siguientes apartados vamos a revisar conceptos teóricos sobre los componentes genéricos de SC, sus pilares fundamentales, la arquitectura y la tecnología usada. Por último, nos enfocamos en la Seguridad en redes IoT, sus aplicaciones y desafíos para nuestro trabajo en este proyecto de investigación que puedan ser transferidos al medio local o regional.

Componentes genéricos de una Ciudad Inteligente

La composición de múltiples atributos o características construyen una ciudad inteligente (ver Fig. 2) y en general son cuatro atributos principales: i) sostenibilidad, ii) calidad de vida, iii) urbanización e iv) inteligencia [11]. A su vez hay atributos secundarios como infraestructura, gobernanza, contaminación y desperdicio, la energía, cambio climático, cuestiones sociales y calidad de vida, economía y salud. Sin embargo, desde el punto de vista tecnológico existen múltiples alternativas para sensores, infraestructura, microcontroladores, interconexión entre componentes, seguridad y sistemas de respaldo que en nuestro proyecto nos ocupa.

Fig. 2 Características generales de SC

En este sentido, podemos afirmar que el entorno, región o ciudad donde se aplique una determinada solución tiene que estar adaptada a diferentes criterios como cultura, estudios de factibilidad técnico-económicos, uso de TICs, normativas locales de uso de telecomunicaciones y espectro, clima, situación política, entre otros aspectos relevantes. Es decir, una solución que funciona en el clima desértico de Dubai puede no ser transferible a ciudades del NEA y viceversa. Es por ello que, en este proyecto se propone estudiar estos conceptos desde el punto de vista académico y proponer soluciones de

sistemas inteligentes basados en seguridad de las comunicaciones, redes definidas por software (SDN) e IoT y que estas soluciones puedan ser transferibles al medio regional.

Pilares fundamentales de una SC

La infraestructura institucional, la infraestructura física, la infraestructura social y la infraestructura económica se consideran los cuatro pilares de una ciudad inteligente [11].

1. La gobernanza de las ciudades inteligentes se enmarca en la infraestructura institucional [12].

Se asocia con la participación en la toma de decisiones, servicios públicos y sociales, gobierno transparente y estrategias y perspectivas políticas. La infraestructura institucional sirve de enlace con los gobiernos regionales y el gobierno central para maximizar los beneficios de la ciudad inteligente. La infraestructura institucional de una ciudad inteligente integra organizaciones públicas, privadas, civiles y nacionales cuando sea necesario.

2. La infraestructura física consiste en recursos naturales e infraestructura fabricada. El pilar de la infraestructura física garantiza la sostenibilidad de los recursos para continuar las operaciones de la ciudad en el presente y en el futuro. Además, la calidad de la infraestructura de las TICs aprovecha el rendimiento de una ciudad inteligente.

3. La infraestructura social de una ciudad inteligente se compone de capital intelectual, capital humano y calidad de vida. La conciencia ciudadana, la responsabilidad y el compromiso juegan un papel clave en la popularización del concepto de ciudad inteligente. Por lo tanto, la infraestructura social se vuelve crucial para la evolución y la sostenibilidad de una ciudad inteligente [13]. Los expertos tanto en la industria como en la academia han declarado que la infraestructura social es un pilar central para cualquier ciudad inteligente debido a su importancia prioritaria.

4. La infraestructura económica de las ciudades inteligentes se refiere al crecimiento económico y al crecimiento del empleo. Además, la economía inteligente se compone de novedosas innovaciones en TIC, fabricación y prestación de servicios relacionados con las TIC, y la integración de tecnologías avanzadas que elevan la confiabilidad y el rendimiento de la gestión [14].

A partir de estos pilares, el despliegue de un Smart City puede medirse en base al índice CIMI [15] que analiza 77 indicadores de ciudades que cubren 10 categorías dominantes en la vida urbana (economía, tecnología, capital humano, cohesión social, alcance internacional, medio ambiente, movilidad y transporte, planificación urbana, gestión pública y gobierno).

Arquitectura y Tecnología en una ciudad inteligente

Actualmente, los investigadores trabajan arduamente en la definición de una aparente arquitectura de ciudad inteligente para mejorar el despliegue de ciudades inteligentes en el mundo real. Sin embargo, la viabilidad de definir una arquitectura universal de ciudad inteligente para el despliegue del mundo real está lejos de la realidad, aunque teóricamente factible. Las variaciones drásticas en las características requeridas restringen la arquitectura universal y hoy no son realistas en muchos escenarios. Sin embargo, en la Fig. 3, luego de un análisis de varias alternativas, proponemos una base de estudio que puede adaptarse a nuestra región.

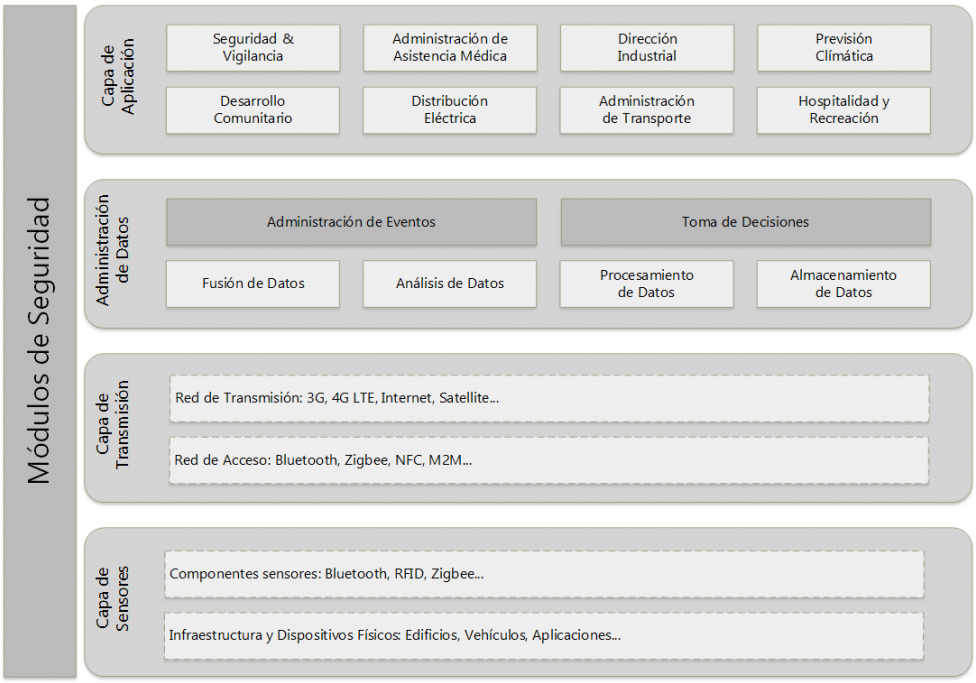

Fig. 3. Arquitectura tecnológica de una SC

Esta arquitectura consta de cuatro capas: (i) capa de sensores, (ii) capa de transmisión de datos o telecomunicaciones, (iii) capa de gestión de datos y (iv) capa de aplicación. Es importante destacar la función clave de la seguridad en los módulos que componen esta arquitectura (v), ya que atraviesa transversalmente a todos los componentes y es materia de estudio en este proyecto de investigación. Los detalles de la tecnología en cada capa son los siguientes:

(i) Capa de Sensores:

Una ciudad inteligente del mundo real se compone de una gran cantidad de datos, cálculos complejos, almacenamiento de información y habilidades inteligentes de toma de decisiones [16]. Para obtener dichos datos, que mayormente son heterogéneos, se adquieren con diferentes dispositivos/sensores de propósito específico como control de electrodomésticos, sensores ambientales, sensores ópticos, etc.

Esta capa captura todos los tipos de datos de todos los tipos de sensores y dispositivos [17]. Por lo tanto, la recopilación de datos desde dispositivos físicos es la principal responsabilidad de la capa de sensores, que reside en la parte inferior de la arquitectura y a través de diversas tecnologías de comunicación, la capa de transmisión transporta datos a las capas superiores. La capa de gestión de datos procesa y almacena información que es útil para la provisión de servicios ofrecidos por varias aplicaciones en la capa superior.

(ii) Capa de transmisión

Para conectar los sensores con las aplicaciones, la capa de transmisión actúa como nexo importante para los sistemas de SC. Esta consiste en varios tipos de tecnologías como redes de cables físicos, inalámbricas y satelitales.

Considerando el aspecto de cobertura, la capa de transmisión se divide además en dos subcapas, transmisión de acceso (corto alcance como Bluetooth, Zigbee, M2M, RFID, Zwave) y transmisión de

red (cobertura más amplia como 3G, 4G (LTE), 5G, y las redes de área amplia de baja potencia, LP-WAN, WI-FI, LI-FI, Fibra óptica) [18].

(iii) Capa de gestión de datos

La capa de gestión de datos es el cerebro de cualquier ciudad inteligente ya que realiza una variedad de tareas de manipulación, organización, análisis, almacenamiento y toma de decisiones de datos [3] De hecho, la eficiencia de la capa de gestión de datos es vital ya que el rendimiento del servicio se basa en la gestión de datos y las operaciones inteligentes de la ciudad se llevan a cabo mediante componentes de administración de eventos y administración de decisiones.

Además, los datos de fuentes heterogéneos se combinan entre sí para ser analizados y aquí se pueden aplicar técnicas de Machine Learning como minería de datos, Big Data [19], etc.

(iv) Capa de aplicación

La capa de aplicación es la capa superior de la arquitectura de SC y está entre los ciudadanos y la capa de gestión de datos. El rendimiento de la capa de aplicación influye en la calidad de percepción del usuario y su satisfacción. Por ejemplo, previsión climática.

La capa de aplicación aumenta el rendimiento de la ciudad a través de numerosas aplicaciones que utilizan datos procesados y almacenados. Sin embargo, la implementación de aplicaciones inteligentes aisladas tiene beneficios mínimos sobre la mejora del rendimiento de las operaciones de la ciudad. Por lo tanto, permitir el intercambio de información entre diferentes aplicaciones parece ser un enfoque prometedor para la evolución de las ciudades inteligentes. Para alcanzar estas demandas, se propone una investigación en términos de desafíos de diseño, optimización del análisis de requisitos, perspectivas de seguridad y estándares.

Seguridad en redes IoT. Aplicaciones y Desafíos

Por último, trataremos en este apartado un aspecto muy importante que vamos a analizar y proponer mejoras en sus aplicaciones en este proyecto y que recorre transversalmente la arquitectura vista anteriormente. Como hemos mencionado anteriormente, los dispositivos de IoT se están volviendo omnipresentes, esto crea nuevos tipos de problemas y preocupaciones de seguridad más complejos.

La seguridad es una necesidad para los sistemas de IoT para proteger los datos confidenciales e infraestructuras físicas críticas [20]. Sin un buen nivel de protección, los usuarios no pueden adoptar muchos sistemas y aplicaciones de IoT. La seguridad en los sistemas de red tradicionales sigue siendo un desafío, mientras que los sistemas de IoT plantean muchos más desafíos a los investigadores debido a varias características especiales de estos sistemas. Un análisis profundo es esencial para desarrollar nuevas soluciones de seguridad y sus aplicaciones a sistemas en nuestra región. Los aspectos que vamos a considerar son:

- Integración con el mundo físico: el acoplamiento plantea preocupaciones de seguridad adicionales ya que el mundo físico ahora puede verse comprometido o controlado a través del mundo tecnológico, lo que podría generar consecuencias extremadamente perjudiciales.
- Dispositivos y comunicaciones heterogéneos: el valor de la tecnología IoT reside en gran medida en su versatilidad y aplicabilidad. Cuando se usan para diferentes dominios de aplicaciones, los sistemas de IoT a menudo adoptan varios dispositivos con hardware y especificaciones de software

dispares. Smart Home como ejemplo, el uso de energía del sistema es monitoreado por sensores de baja capacidad que solo pueden realizar cálculos simples y proporcionar lecturas esporádicas. Por el contrario, los sistemas de vigilancia de la seguridad del hogar deben proporcionar monitoreo del área del hogar en tiempo real.

- Restricciones de recursos: Para reducir el costo de desarrollo y fabricación, los proveedores a menudo equipan los dispositivos IoT con capacidades limitadas. Esto da como resultados dispositivos de baja capacidad con diversas limitaciones de recursos, como espacio de memoria pequeño, capacidad de cálculo baja, ancho de banda de comunicación bajo y suministro de alimentación limitado. Por ejemplo, un dispositivo IoT típico puede ejecutar un sistema de 8 bits o 16 bits. Estas restricciones de recursos contribuyen directamente a muchas de las inseguridades de IoT porque las soluciones de seguridad tradicionales a menudo no pueden funcionar en dispositivos de baja capacidad.
- Privacidad: Como los sistemas de IoT a gran escala a menudo generan, recopilan y analizan grandes volúmenes de datos para obtener inteligencia, la privacidad se convierte en una gran preocupación. Cuando se usa en un dominio médico, IoT puede representar una amenaza para la privacidad de la información médica de las personas. Cuando se usa en un hogar inteligente, IoT puede exponer la vida personal de uno al mundo exterior, que puede ser potencialmente peligroso.
- La gran escala: La escala cada vez mayor complica los desafíos del diseño de soluciones de seguridad para los sistemas de IoT. En primer lugar, la gran cantidad de interacción entre todos los dispositivos aumenta significativamente el costo de implementación de seguridad. En segundo lugar, es difícil aplicar esquemas de gestión que ya tienen problemas de escalabilidad a sistemas de IoT a gran escala [21]. En tercer lugar, la administración del sistema posterior a la implementación también será un gran desafío [22]. Por ejemplo, es posible que las personas no vean los dispositivos de IoT (como televisores, heladeras, etc.) como dispositivos que implican la informática y deben protegerse.
- Gestión de confianza: La confianza es un componente esencial en el diseño de seguridad [23]. Con una gran parte de los sistemas de IoT organizados como redes peer-to-peer o ad hoc, la gestión de confianza sigue siendo un desafío importante en IoT, ya que es un tema desafiante en cualquier red [24]. Además, la alta movilidad, la ausencia de identidad global y la relación temporal entre los dispositivos de IoT complican aún más el diseño de una solución de confianza eficiente.
- Diseño de la seguridad: se refiere al análisis de ingeniería sobre las cuestiones de seguridad de los dispositivos en sí y las redes que comunicarán a éstos. Sin considerar estos aspectos, los atacantes pueden acceder sin autorización a los dispositivos mediante el uso de técnicas de piratería simples.

Si esos problemas de seguridad no pueden abordarse adecuadamente, se dificultará en gran medida una adopción más amplia de las aplicaciones de la IoT.

Lo que nos preguntamos hoy en este sentido es… ¿Por qué la seguridad es más desafiante en IoT y qué aspectos serán relevantes para nuestro proyecto?

Resultados, Avances/Discusión

Los resultados obtenidos en el proyecto podrán ser utilizados en las siguientes áreas del conocimiento:

A) Arquitecturas de redes de Información para IoT. El relevamiento y análisis de las nuevas tendencias de redes de información de corto y amplio rango, conllevará a publicaciones científicas y transferencias al medio local o regional. Esto propiciará el contacto con investigadores de nivel internacional y nacional de otras instituciones para posibles intercambios de experiencias como el que se está llevando a cabo con el proyecto REMIND de la Unión Europea.

B) Programación y pruebas de diversos dispositivos usados para IoT y ciudades inteligentes como sensores y equipos de telecomunicación entre ellos sin intervención humana y que ayude a la toma de decisiones y mejore la gestión que lo utilice.

Una vez finalizado el proyecto generará nuevo conocimiento y aplicaciones que pueden ser transferidos tanto a entornos de investigación como diferentes entornos organizacionales o empresas del medio. En este sentido se pretende impulsar el intercambio de conocimiento con investigadores de otras instituciones, asistencia a eventos científicos, elaboración de publicaciones científicas, estancias de investigación en el exterior, convenios de transferencia, etc.

En cuanto a las transferencias al medio existen dos líneas abiertas:

A) El primer sistema se basa en crear una red de estudio meteorológico y ambiental sobre 42 puntos distribuidos en toda la provincia. La medición se hará en los nodos de fibra óptica provinciales y los datos serán enviados a un centro de procesamiento en la ciudad de Resistencia.

B) Sistemas de Telecomunicación con LORA y dispositivos IoT mediante convenio a realizarse con la empresa YEAP. Dicha empresa proveerá soporte de antenas y software de prueba académicos.

Referencias

[1] Sekhar N. Kondepudi, et. al. An overview of smart sustainable cities and the role of information and communication technologies. Set of ITU-T's Technical Reports and Specifications. 2016.

[2] Bhagya Nathali Silva, Murad Khan, Kijun Han. Towards sustainable Smart Cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society. 38. 2018

[3] Silva, B. N., Khan, M., & Han, K. Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. IETE Technical Review, 1–16. 2017.

[4] Silva, B. N., Khan, M., & Han, K. Big data analytics embedded Smart City architecture for performance enhancement through real-time data processing and decision-making. Wireless Communications and Mobile Computing. 2017.

[5] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29, 1645–1660. 2013.

[6] Vermesan, O., Friess, P., Guillemin, P., Giaffreda, R., Grindvoll, H., Eisenhauer, M., et al. Internet of things beyond the hype: Research innovation and deployment. IERC Cluster SRIA. 2015.

[7] Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. The Internet of Things for Healthcare: A comprehensive Survey. IEEE Access, 3, 678–708. 2015.

[8] Hollands, R. G. Will the real Smart City please stand up? Intelligent, progressive or entrepreneurial city?, 12, 303–320. 2008.

[9] Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., et al. Foundations for smarter cities. IBM Journal of Research and Development, 54, 1–16. 2010.

[10] Kondepudi, S. Smart sustainable cities analysis of definitions. The ITU-T Focus Group for Smart Sustainable Cities. 2014.

[11] Mohanty, S. P., Choppali, U., & Kougianos, E. Everything you wanted to know about smart cities: The internet of things is the backbone. IEEE Consumer Electronics Magazine, 5, 60–70. 2016.

[12] The Government Summit. Smart Cities: Regional Perspectives. The Government Summit. 2015.

[13] Nam, T., & Pardo, T. A. Conceptualizing smart city with dimensions of technology, people, and institutions. Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times ACM, 282–291. 2011.

[14] Lombardi, P., Giordano, S., Farouh, H., & Yousef, W. Modelling the smart city performance. Innovation: The European Journal of Social Science Research, 25, 137–149. 2012.

[15] Berrone, P. R., & Enric, J. IESE cities in motion index. IESE Business School University of Navarra. 2016.

[16] Wenge, R., Zhang, X., Dave, C., Chao, L., & Hao, S. Smart city architecture: A technology guide for implementation and design challenges. China Communications, 11, 56–69. 2014.

[17] Deshpande, A., Guestrin, C., Madden, S. R., Hellerstein, J. M., & Hong, W. Model-driven data acquisition in sensor networks. Proceedings of the Thirtieth international conference on Very large data bases-Volume 30. VLDB Endowment, 588–599. 2004.

[18] Sanchez-Iborra, R., & Cano, M.-D. State of the art in LP-WAN solutions for industrial IoT services. Sensors, 16, 708. 2016.

[19] Kitchin, R. The real-time city? Big data and smart urbanism. Geo Journal, 79, 1–14. 2014.

[20] K. Sha, W. Wei, A. Yang, W. Shi. Security in Internet of Things: Opportunities and challenges. Proceedings of International Conference on Identification, Information & Knowledge in the Internet of Things (IIKI). 2016.

[21] J. Qi, et al. Security of the Internet of Things: Perspectives and challenges, Wirel. Netw. 20 (8) 2481–2501. 2014.

[22] Z. Wan, et al. SKM: Scalable Key Management for advanced metering infrastructure in smart grids, IEEE Trans. Ind. Electron. 61 (12) 7055–7066. 2014.

[23] Z. Yan, P. Zhang, A.V. Vasilakos. A survey on trust management for Internet of Things, J. Netw. Comput. Appl. 42 (4) 120–134. 2015.

[24] Q. Han, H. Wen, G. Feng, B. Wu, M. Ren. Self-nominating trust model based on hierarchical fuzzy systems for peer-to-peer networks, Peer-to-Peer Netw. Appl. 9 (6) 1020–1030. 2016.