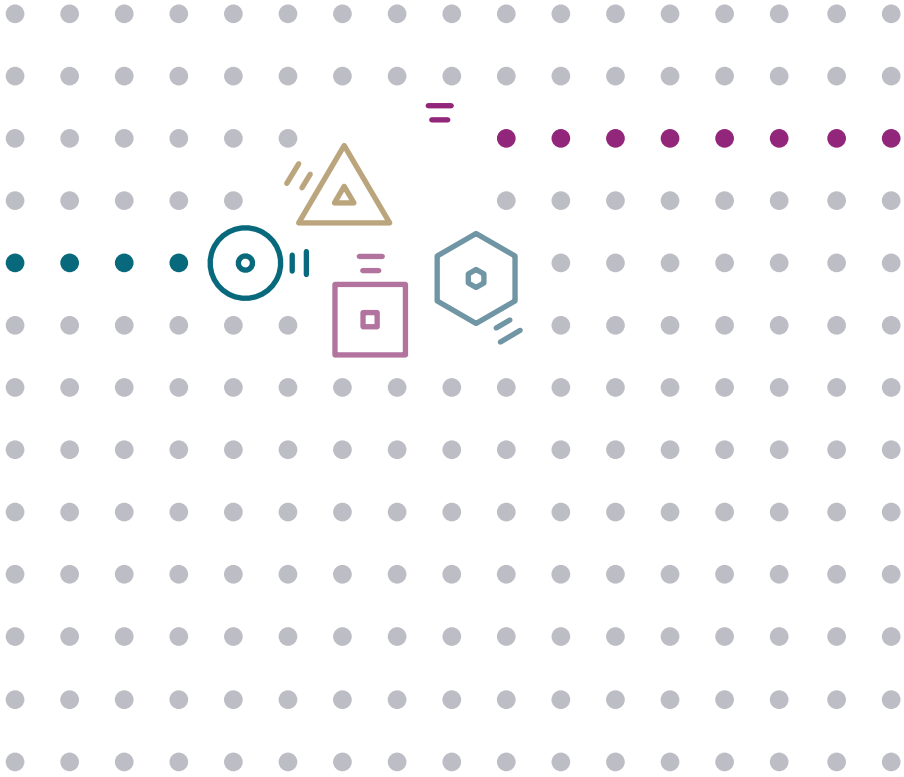
Internet de las cosas (IoT)

Retos sociales y campos de investigación científica en relación con la IoT



Inria | LIBRO BLANCO | N°05

Este documento ha sido redactado y coordinado por Emmanuel Baccelli.

***Contribuciones** – Gracias a las siguientes personas por sus sugerencias y aportaciones textuales: N. Anciaux, K. Bhargavan, G. Casiez, F. Gandon, N. Georgantas, J.M. Gorce, S. Huot, E. Lank, A. Lebre, W. Mackay, K. Marquet, N. Mitton, E. Rutten, M. Tommasi, P. Vicat-Blanc, O. Sentieys, B. Salvy, M. Serrano, B. Smith, M. Vucinic, T. Watteyne.*

***Agradecimientos** – Gracias a las siguientes personas por sus útiles comentarios: C. Adjih, C. Bormann, I. Chrisment, F. Cuny, F. Desprez, MA Enard, JF Gerbeau, P. Guitton, V. Issarny, P. Jacquet, L. Mé, V. Roca, H. Tschofenig, A.Viana.*

Del original:
Emmanuel Baccelli. Internet of Things (IoT): Societal Challenges & Scientific Research Fields for IoT. 2021. hal-03474888
1º Edición
Fecha de publicación: Noviembre 2021, Francia

Traducción autorizada del idioma inglés de la edición publicada por Inria

Traducción al español realizada por Inria Chile

Coordinación general y revisión técnica: Nayat Sánchez Pi

Coordinación de producción: Julia Allirot y Katherine Lippi

Coordinación ejecutiva: Andrés Vignaga

Revisión gráfica y maquetación: Mia Elbo y Katherine Lippi

***Agradecimientos** – Gracias a las siguientes personas de Inria Chile por sus aportes a la revisión técnica: Jaime Aranda, Andrés Vignaga*

Impreso por Lahosa
Impresión: Octubre 2022, Chile
ISBN: 978-956-09873-2-7

Impreso en Chile / Printed in Chile

Índice

Resumen ejecutivo

Del mismo modo que la Internet transformó radicalmente la sociedad, la Internet de las cosas (*Internet of Things* o IoT por sus siglas en inglés) repercutirá en todos los ámbitos de la vida humana: desde nuestros hogares, vehículos, lugares de trabajo y fábricas, hasta nuestras ciudades y pueblos, la agricultura y los sistemas sanitarios. También afectará a todos los niveles de la sociedad (individuos, empresas y estado), desde lo urbano hasta lo rural, pasando por el mundo natural y más allá. Por ello, es fundamental tener un conocimiento adecuado de la IoT y de los retos que conlleva. Los objetivos principales de este documento son:

- determinar el alcance de la IoT, sus orígenes, su evolución actual y sus perspectivas;
- identificar los principales retos sociales, técnicos y científicos relacionados con la IoT.

Todo parece indicar que la IoT será cada vez más ubicua. De hecho, está destinada a penetrar en todos los aspectos de nuestra vida, conectando (miles de millones de nuevas máquinas heterogéneas que se comunican entre sí) y midiéndolo todo: desde la acción colectiva que realizamos a nivel global, hasta nuestras más pequeñas señales fisiológicas individuales, en tiempo real. Se trata de un arma

de doble filo, ya que al mismo tiempo da motivos de esperanza (automatización, optimización, nuevas funcionalidades innovadoras, etc.) y de temor (vigilancia, dependencia, ciberataques, etc.). Dada la constante evolución de la IoT, aparecen nuevos retos relacionados con la privacidad, la transparencia y la seguridad, al tiempo que empiezan a surgir nuevas responsabilidades civiles e industriales.

La IoT se centra en un conjunto cada vez más complejo de conceptos interconectados y tecnologías embebidas. A nivel industrial, esta creciente complejidad está haciendo que la idea de tener un control total sobre todos los componentes de la IoT sea cada vez más difícil, o incluso inviable. De todos modos, es importante que a nivel de sociedad todos nos familiaricemos con los fundamentos tecnológicos de la IoT. Por lo tanto, uno de los desafíos de la educación será el aumento gradual sobre la sensibilización sobre la IoT, tanto para proteger la soberanía y el libre albedrío de los individuos, como para iniciar la formación de nuestros futuros científicos y técnicos. Un instituto público de investigación tal como Inria puede contribuir a entender y explicar los fundamentos tecnológicos de la IoT, además de preservar la soberanía en Europa.

La IoT inevitablemente hará que aumente la dependencia sobre ciertos tipos de tecnología embebida. Por lo tanto, se deben identificar los nuevos riesgos que conlleva, y diseñar nuevas estrategias para aprovechar al máximo la IoT, al tiempo que se minimicen estos riesgos. Al igual que ocurre en otros ámbitos, en los que se debe procurar constantemente proteger la ética sin obstaculizar la innovación, la creación de un marco jurídico para la IoT es necesaria y desafiante a la vez. No obstante, se ve que la mejor manera de enfrentarse a los gigantes o superpotencias industriales es actuar a nivel de la UE, y así lo demuestran iniciativas recientes como el reglamento de protección de datos (GDPR, por sus siglas en inglés). Además, dada la creciente influencia de las normas tecnológicas en la sociedad, es imprescindible desempeñar un papel activo en el proceso de normalización de la tecnología de la IoT. Los estándares y el código abierto —concebidos como un bien público común— serán fundamentales para la IoT, tal y como lo han sido para Internet. Finalmente, aunque no menos importante, el uso masivo de la IoT puede ayudar a captar y comprender mejor los retos medioambientales a los que nos enfrentamos en la actualidad; también se espera que la IoT ayude a mitigar estos desafíos. Los objetivos en este contexto no son sólo reducir las cantidades de recursos naturales que consume la IoT (en cuanto a su producción, despliegue, mantenimiento y reciclaje). Debemos también tratar de evaluar con mayor precisión el beneficio neto general de la IoT en el medio ambiente, a nivel global. Para ello es necesario determinar y restar los costos medioambientales

de la IoT de sus beneficios (medidos), lo que constituye un reto en la actualidad. El creciente impacto de la IoT pone de manifiesto la importancia de mantenerse a la vanguardia de la investigación científica y el desarrollo tecnológico. Por lo tanto, este documento pretende:

- destacar la amplia gama de campos de investigación que son fundamentales para la IoT;
- hacer un balance de los problemas actuales y futuros de la investigación en cada uno de estos campos.

A lo largo del documento se incluye una serie de enlaces a las contribuciones de Inria. Por naturaleza, estas contribuciones son diversas (investigación básica y aplicada, software de código abierto, incubación de startups) y afectan a la mayoría de los campos de investigación en los que se basa la IoT.

PRÓLOGO: *El capullo de Alicia*

El sueño de Alicia

Alicia valora su libertad. Si Alicia lo desea, sus dispositivos vestibles, prendas e implantes inteligentes (que combinan sensores, actuadores y comunicaciones inalámbricas locales) de Alicia colaboran entre sí. Alicia también puede interconectar fácilmente sus dispositivos con otros dispositivos inteligentes cercanos, o con recursos informáticos más remotos de su elección, accesibles a través de la red cuando sea necesario. Todo el sistema proporciona a Alicia un manto ciberfísico personal que "amortigua" su experiencia dondequiera que esté: en casa, de viaje o en el trabajo.

De camino a su lugar de trabajo en la fábrica, el vehículo autodirigido de Alicia interactúa con la infraestructura de la ciudad inteligente para tomar automáticamente la ruta menos congestionada, según las preferencias de Alicia, y para localizar una plaza de aparcamiento cerca de la fábrica donde trabaja. El mantenimiento predictivo y la supervisión avanzada del entorno en tiempo real que se utilizan en la fábrica garantizan un lugar de trabajo seguro y productivo, al tiempo que se optimiza el consumo de energía. Ya de vuelta en casa, el capullo de Alicia sigue personalizando su experiencia ciberfísica al orquestar la interacción con sus aparatos. Sobre todo: Alicia sigue manteniendo el control y puede confiar en el sistema, que funciona de forma segura, protegiendo su privacidad.

Por ejemplo, Alicia utiliza su capullo para proporcionarle una asistencia sanitaria predictiva avanzada. Si Alicia lo desea, puede desactivar el sistema y borrar los datos en cualquier momento a través de una interfaz sencilla pero significativa, y puede intercambiar fácilmente los dispositivos o los recursos informáticos remotos. Puede captar los aspectos clave del sistema en el trabajo y autoevaluar su estado de salud, por ejemplo, informarse sobre posibles síntomas de alerta. Si Alicia lo desea, puede optar por compartir algunos de sus datos sanitarios con su médico, de forma temporal o permanente. Si lo solicita, el capullo electrónico de Alicia también puede participar activamente en tratamientos médicos avanzados o en la prevención coordinada de la propagación de determinados virus.

De este modo, Alicia se puede beneficiar de la mejor salud, de forma voluntaria, y con un costo optimizado para ella, para su empleador y para la sociedad en general. Y todo esto, ¡mientras Alicia se acaba de mudar a un lugar apartado en el campo!

La pesadilla de Alicia

El taxi autodirigido de Alicia la estrelló contra un árbol. La empresa de taxis aclaró posteriormente que su flota de vehículos se vio afectada por señales de GPS falsas. Por suerte, Alicia no sufrió lesiones graves, pero uno de sus preciados implantes inteligentes se rompió con el golpe. Lograr que su capullo electrónico funcionara correctamente (tras cambiar el dispositivo por uno de repuesto) tardó mucho más de lo que Alicia había previsto. Además, para colmo de males, Alicia debe pagar urgentemente un cuantioso rescate debido a que su otro implante inteligente fue hackeado: los piratas habían explotado a distancia las vulnerabilidades de su software.

Ahora Alicia se ve forzada a recortar sus gastos. La compañía de seguros, que pretende optimizar el riesgo y las utilidades, exige a Alicia que acceda a utilizar dispositivos adicionales de seguimiento de sus signos vitales y que consienta la venta de sus datos a terceros. La privacidad de Alicia disminuye drásticamente. Superando la ficción Orwelliana, el comportamiento de Alicia se rastrea minuciosamente en tiempo real, y varios actuadores distorsionan visiblemente su realidad.

A nivel laboral, Alicia es espiada constantemente por sus superiores, que abusan de las capacidades de seguimiento y actuación de la infraestructura de IoT de la fábrica, que a su vez son objeto de ciberataques cada vez más frecuentes, lo que pone en peligro la productividad y la seguridad en su lugar de trabajo. En su vida "privada", Alicia es presa del capitalismo de vigilancia avanzada; su comportamiento se ve a menudo influido a través de su capullo ciberfísico por diversas entidades con fines de lucro.

Tras un estudio piloto, el gobierno propone una nueva política que generaliza el uso obligatorio del seguimiento sanitario a través del capullo electrónico, con la intención de disminuir la deuda pública del país. Esta reforma se discute en medio de la creciente sospecha de que las recientes elecciones estuvieron influenciadas por perfiles avanzados que utilizan datos de seguimiento de la salud en tiempo real, y que se aprovechan para manipular a los votantes a escala masiva...

La conectividad ubicua y la dependencia tecnológica fabricada hacen imposible que Alicia escape a las garras de la ciudad inteligente. Alicia se siente perdida, aprisionada en su capullo electrónico, preguntándose qué le queda de su intimidad, y de hecho de su propia voluntad, en esta sociedad de locos.

Cómo fomentar el optimismo y reducir el pesimismo en el ámbito de la IoT

La realidad de Alicia aprovecha la Internet de las Cosas (IoT), que es motivo de optimismo y pesimismo a varios niveles, y que crea simultáneamente nuevas oportunidades y plantea nuevos problemas. Aunque no todos estos problemas tienen una solución técnica, sin duda la ciencia y la tecnología pueden contribuir a disminuir los posibles efectos negativos. Para facilitar el optimismo de la IoT y reducir las causas del pesimismo, la tecnología debe combinar los avances en diversos campos científicos, tales como:

- redes informáticas (para que los dispositivos de Alicia se comuniquen e interactúen),
- hardware miniaturizado de bajo consumo (para que los dispositivos de Alicia sean duraderos y cómodos de llevar),
- software embebido de bajo consumo (para que los dispositivos puedan cooperar, de forma duradera, con una batería pequeña),
- informática distribuida (para que Alicia mantenga la flexibilidad en cuanto a dónde y cómo se pueden procesar sus datos),
- procesamiento de datos que protege la privacidad (para que Alicia pueda controlar los datos personales o sensibles, y gestionar su uso),
- control y robótica (para dirigir eficazmente los sensores y actuadores de Alicia),
- Interfaz humano-máquina (que permite un control sencillo pero potente del sistema),
- la seguridad del sistema (que garantice que los actuadores no sean peligrosos para Alicia o para otras personas), y
- la protección del sistema (para defender a Alicia de posibles piratas informáticos).

Inria, con sus más de 200 equipos de proyectos en ocho centros de investigación, trabaja en todas estas áreas científicas. Este documento expone la visión de Inria sobre las principales tendencias y retos de la IoT, y cómo sus equipos están llevando a cabo activamente la investigación científica, el desarrollo de software y la transferencia de tecnología en torno a estos retos.

Extendiéndose a otros ámbitos, este documento también identifica los principales retos sociales en un mundo que depende de la IoT, que van desde cuestiones éticas hasta la transparencia, la soberanía y la educación.

Una serie de reportes técnicos han abordado aspectos de la IoT con anterioridad. Algunos se han centrado principalmente en subtemas de la IoT, por ejemplo, en los aspectos relacionados con las telecomunicaciones y la regulación (ver reportes ARCEP o AFNIC), o sobre el software de código abierto para la IoT (ver reporte de Systematic). Sin embargo, otros han analizado la IoT desde el punto de vista de los proveedores de hardware industrial (ver el reporte de NXP), o desde el punto de vista del proveedor de servicios informáticos (ver el reporte de Atos). En este documento, en cambio, se presenta una cobertura fundamentalmente integral de la Internet de las Cosas, anclada en torno a los desafíos de la investigación científica que atañen a la IoT.

PARTE I

La Internet de las Cosas (IoT)

En esta primera parte, comenzamos a analizar la IoT, su nacimiento, su estado actual y sus perspectivas. Luego, identificamos los desafíos sociales, técnicos y científicos relacinados a la IoT

1

IoT: Pasado, presente y perspectivas

Más allá del término de moda, **resulta difícil definir la IoT.** Efectivamente, los aspectos de la IoT abarcan desde el hardware hasta el software, desde las tecnologías de red hasta la ciencia de los datos, desde los servicios hasta el despliegue de infraestructuras, desde las redes de sensores inalámbricas hasta la computación en la nube. ¿Sigue siendo la IoT una quimera? ¿O ya está sucediendo? ¿Qué es la IoT? Las respuestas a estas preguntas son numerosas y discutibles, al igual que las respuestas a la pregunta "¿qué es Internet?

En este documento, consideramos la IoT como la encarnación de una parte importante de la Internet del futuro. En este sentido, la IoT se compone de un conjunto de tecnologías de uso general que:

- cierra la brecha entre el mundo digital y el físico;
- cierra la brecha entre las tecnologías de Internet y una variedad cada vez mayor de sistemas embebidos.

La terminología de la IoT no está del todo establecida. En este documento consideramos que la IoT equivale, a grandes rasgos, a lo que se denomina *Internet de todo* (terminología de Cisco/W3C), la *Web Física* (terminología de Google), *Computación Física* (terminología de Arduino), *Maquina-a-Máquina* (M2M), los *Sistemas Ciberfísicos* (terminología de la teoría del control) o la *World-Sized Web* (término acuñado por B. Schneier).

Breve Prehistoria de la IoT

Incluso antes de la Internet, ya habían empezado a aparecer en el mercado productos de domótica como el X10. Luego, a principios de los años 90, visiones futuristas como el Escritorio Digital (Digital Desk) imaginaban "objetos aumentados" que cooperaban a través de la red e interfaces para interacciones tangibles que difuminaban la frontera entre el mundo digital y el físico. Al mismo tiempo, la IoT también se anticipó a visiones como la de Mark Weiser sobre la computación ubicua y la virtualidad encarnada (ubiquitous computing and embodied virtuality), que poco a poco se está haciendo realidad.

A finales de los años 90, el Centro de Identificación Automática fue pionero en la aparición de las etiquetas RFID, augurando un mundo en el que prácticamente todos los objetos se podrían identificar y direccionar de forma exclusiva a través de la red. En este sistema preliminar, cada etiqueta contaba con un microchip sencillo que sólo almacenaba un número de serie básico (para abaratar costos)

que se podía consultar en las inmediaciones mediante una conexión inalámbrica local. Los datos asociados al número de serie de la etiqueta se almacenaban por separado en una base de datos accesible en línea.

En la década de los 2000, surgieron nuevos conceptos y técnicas que permitieron la creación de redes inalámbricas de sensores y actuadores (WSAN o WSN): diminutos computadores alimentados por baterías que primero colaboran para establecer redes inalámbricas (de varios saltos) y luego utilizan dichas redes para transportar los datos de sus sensores o para distribuir los comandos de los actuadores.

Para generalizar estos conceptos, se introdujo el término "informática omnipresente" (algo parecido a la informática ubicua) para captar la tendencia a integrar algunas capacidades informáticas y de comunicación en los objetos cotidianos. La expresión "Internet de las cosas" se comenzó a emplear de forma generalizada en la década de los 2010.

Desde entonces, a lo largo de la última década, han aparecido diversos objetos aumentados que ofrecen diferentes niveles de potencia de cálculo y cooperación en la red.

Red de sensores FIT/IoT Lab instalada en el centro de investigación Inria Grenoble Rhône-Alpes.
© Inria / Photo H. Raguet.

La innovación que favorece el surgimiento de la IoT

La aparición de la IoT se ha visto acelerada recientemente por la innovación en los ámbitos del hardware embebido de bajo consumo, las redes de bajo consumo, el software de sistemas embebidos y la informática de borde o periférica (edge computing). Una amplísima variedad de actores industriales (PYMEs y grandes empresas tecnológicas) contribuyen a innovar en estos ámbitos, a distintos niveles. Han surgido tanto nuevas organizaciones de desarrollo de estándares (SDO, por sus siglas en inglés) como nuevos estándares tecnológicos de la IoT. Para los lectores interesados, ofrecemos referencias concretas: esta lista no es ni mucho menos exhaustiva, ya que nuestro objetivo no es establecer la relevancia, sino ilustrar la diversidad de esta innovación.

Innovación en hardware embebido

Por un lado, se han masificado los computadores económicos de placa única (por ejemplo, RaspberryPi, NVIDIA Jetson Nano, etc.). Por otro lado, proveedores como STMicroelectronics, Microchip Technology Inc, Espressif o SiFive han desarrollado nuevo hardware para dispositivos IoT de muy bajo consumo, con novedosas arquitecturas de microcontroladores diseñadas por empresas como ARM Ltd., o estándares de hardware de código abierto como RISC-V. Asimismo, empresas como NXP Semiconductors o Nordic Semiconductors, por ejemplo, proporcionan nuevos coprocesadores de seguridad y criptografía de bajo consumo.

Innovación en redes de bajo consumo

Los dispositivos más pequeños, como los sensores/actuadores, se conectan en red utilizando nuevas radios de baja potencia (por ejemplo, LoRa, 802.15.4, BLE, etc.), diminutas pilas de protocolos de red de uso general (por ejemplo, 6LoWPAN) y un conjunto casi infinito de direcciones de red únicas (con IPv6). Están apareciendo equipos de comunicación sin batería y que cosechan energía, encabezados por empresas como EnOcean y Onio. Consorcios y SDOs como la Alianza LoRa, el IEEE, el IETF, el W3C o el 3GPP producen nuevas especificaciones abiertas para el protocolo de comunicación de redes que se adaptan a los dispositivos de baja potencia. Empresas como Semtech y Texas Instruments proporcionan nuevos chips de radio de bajo consumo que utilizan los proveedores de hardware y los nuevos operadores centrados en la IoT, como Sigfox o Actility, o los grandes operadores tradicionales, como Orange, SFR o Bouygues.

Innovación en software embebido

Las distribuciones compactas embebidas de Linux se han convertido en las plataformas de software más destacadas para los equipos de placa única (dispositivos IoT de gama alta basados en microprocesadores), para los que un amplio grupo de desarrolladores de pequeñas y grandes empresas contribuyen con código abierto. En los dispositivos más pequeños (dispositivos de IoT de gama baja basados en microcontroladores), las nuevas plataformas de software de sistemas de código abierto embebidos agregan el desarrollo de software de bajo consumo, por ejemplo, FreeRTOS (Amazon), Zephyr (Intel), Arduino o RIOT.

Innovación en informática de borde (edge computing)

Esta tendencia pretende acercar físicamente la informática y el almacenamiento de datos a las fuentes de información. Los nuevos ecosistemas aceleran el despliegue, la operación y el mantenimiento de la informática de borde. Por ejemplo, las plataformas como TFLite, dirigida por Google, facilitan el desarrollo de software de aprendizaje automático embebido. Los novedosos coprocesadores de hardware y el software proporcionados por empresas como ARM, o Greenwaves Technologies, mejoran las capacidades operativas mediante el uso de redes neuronales en los dispositivos IoT situados en el borde de la red. La informática de borde también se ve facilitada por nuevas herramientas de gestión de código abierto dedicadas a la IoT, tales como las que desarrolla la Eclipse IoT Foundation, o por herramientas de gestión de flotas como Kubernetes. Los servicios en la nube atienden a la IoT y la informática de borde con servicios adaptados como los que proporcionan Microsoft Azure IoT Hub o Amazon IoT GreenGrass.

A medida que esta innovación se integra más fácilmente con las tecnologías genéricas de Internet, y con la infraestructura común de la nube, el despliegue de la IoT irá en auge.

Aparte de su actividad investigadora, Inria también ha desarrollado marcos de apoyo para proyectos de Tecnología Profunda (Deep Tech) que innovan aplicando los resultados de la investigación. De hecho, **Inria incuba e impulsa a las pymes** con su programa Startup Studio. Algunos ejemplos recientes de este tipo de empresas derivadas relacionadas con el ámbito de la IoT son, por ejemplo, Falco, Stackeo, Statinf o CryptoNext.

FALCO es una empresa que proporciona hardware, software y servicios de IoT que ayudan a la gestión medioambiental de los puertos deportivos: seguimiento en tiempo real de los muelles disponibles, control optimizado de los recursos,

lucha contra la contaminación y sensibilización sobre las buenas prácticas. Los productos de Falco aprovechan, entre otras cosas, la tecnología de IoT inalámbrica de bajo consumo desarrollada por los investigadores de Inria.

STACKEO es una empresa de software derivada de Inria, que ayuda a las empresas a industrializar sus soluciones de conectividad e IoT a escala. A partir de un modelo de negocio de software como servicio, Stackeo ofrece un conjunto de herramientas que permiten articular una estrategia de IoT, alinear los equipos de IoT y pilotar cadenas de valor sostenibles. Stackeo desarrolla el concepto de IoT-Architecture-as-Code (Arquitectura IoT como código), a partir de un lenguaje de modelado específico y en una metodología sistémica patentada.

STATINF es una empresa que proporciona herramientas que permiten el análisis estadístico del comportamiento temporal del software embebido, para sistemas en tiempo real con procesadores multinúcleo. Con este tipo de herramientas, los sistemas embebidos altamente críticos de sectores como la aviónica, la automoción, los drones o el sector aeroespacial pueden interpretar las posibles variaciones en el tiempo de ejecución del software que utiliza su hardware de IoT embebido.

CRYPTONEXT es una empresa de ciberseguridad surgida de Inria y la Universidad de la Sorbona, que proporciona bibliotecas de software que implementan algoritmos criptográficos diseñados y optimizados para la seguridad post-cuántica. CryptoNext también ofrece consultoría en el ámbito de la ciberseguridad resistente a la tecnología cuántica.

La IoT en la actualidad: el punto de inflexión

Consideremos que los dispositivos IoT pueden ser cualquier tipo de dispositivos conectados tanto de consumo como B2B, excluyendo los teléfonos, las tabletas y los computadores portátiles/de escritorio. Luego, entre 2010 y 2020, el número de dispositivos IoT conectados ha crecido nada menos que en un asombroso 1.000%. En la última década se desplegaron e interconectaron aproximadamente 10.000 millones de dispositivos IoT. Para tener una visión global sobre esta evolución: en 2010, la proporción de IoT entre los dispositivos conectados era del 10%. En 2020, esta proporción aumentó a más del 50%: en otras palabras, ya se ha superado el punto de inflexión. A partir de ahora, los dispositivos IoT superan oficialmente a los que no lo son. Los análisis del mercado mundial informan que en 2019, la IoT generó más de 300.000 millones de dólares en ingresos a nivel mundial, una cifra que crece cada vez más.

Muchos dispositivos IoT dependen de microcontroladores de bajo consumo. Se despacharon más de 28 mil millones de microcontroladores en 2018, y se estima que se usaron alrededor de 250 mil millones de microcontroladores en todo el mundo el 2020. No todos los microcontroladores están conectados en red, pero hay cada vez más despliegues que dependen tanto de microcontroladores con códigos cada vez más complejos y que están conectados a una red ya sea directa o indirectamente. La mayoría se conecta a través de redes inalámbricas personales, locales, de área amplia o celulares. Estos despliegues proliferan en una amplísima variedad de segmentos, entre los que se encuentran (en orden decreciente según su cuota de mercado): las aplicaciones automotrices, la automatización industrial, los dispositivos de consumo personal/doméstico, los contadores inteligentes en los sistemas de redes inteligentes, las aplicaciones sanitarias y los ámbitos aeroespacial y de defensa. En el segmento industrial, por ejemplo, la red se extiende a una multitud de procesos que tradicionalmente dependían de bucles de control locales de sensores/actuadores. Los datos agregados en tiempo real y los "gemelos digitales" tienen como objetivo hacer un análisis minucioso de la totalidad de las complejas cadenas de suministro, producción y venta, y controlarlas globalmente.

Perspectivas de la IoT: Miles de nuevas formas de percibir y actuar

Los despliegues de IoT están previstos en prácticamente todos los mercados y verticales: hogar inteligente, edificios de energía neta cero, asistencia sanitaria electrónica, Industria 4.0, agricultura de precisión, vigilancia de la fauna y el medio ambiente en tiempo real, ciudades inteligentes, cadena de suministro de transporte de mercancías, uso compartido de coches/bicicletas/motocicletas, etc. En lugar de intentar enumerarlos exhaustivamente, los lectores que se interesen en estos temas pueden consultar estas referencias. Según las proyecciones, decenas de miles de millones de dispositivos IoT adicionales se desplegarán por todo el planeta, interactuando a través de la red, eclipsando las conexiones no IoT en un futuro cercano.

Básicamente, la IoT dota a Internet de extremidades. La IoT despliega nuevas formas de comunicación, de adquisición (recopilación de datos), de razonamiento (uso de estos datos) y de actuación física a través de actuadores. Si fuera necesario, las nuevas variedades de bucles de control a través de la red pueden aprovechar grandes recursos informáticos remotos. Al comprender/asimilar y explotar estos nuevos bucles de control, la IoT está transformando drásticamente el panorama:

• Los **sensores** se utilizan para observar los procesos de forma más cercana y precisa. Por ejemplo, los sensores pueden captar las ineficiencias de los sistemas complejos, con el fin de reducir drásticamente los gastos operativos. Los líderes de la IoT industrial proyectan que los procesos industriales se pueden optimizar combinando el hardware industrial, la conectividad inalámbrica de la IoT y una sofisticada canalización de datos: los problemas y las averías se pueden detectar mucho más rápido (en minutos u horas, en lugar de días o semanas con las prácticas actuales), lo que permite reducir las pérdidas en cientos de miles de dólares al año por planta, y generar un crecimiento de dos dígitos en la producción y los beneficios brutos mediante el aumento de la velocidad de la línea en estado estacionario.

Los **actuadores** permiten una (re)configuración rápida, adaptable y automatizada de sistemas ciberfísicos complejos. Por ejemplo, las estrategias autónomas de ahorro de energía se pueden instalar en varios niveles (por ejemplo, un complejo de edificios o una ciudad entera) y pueden interactuar dinámicamente para lograr una disminución drástica del consumo de energía. También se prevé que la mejora en la reducción de nuestro impacto ambiental, gracias a la detección de la contaminación y la sensibilización sobre el consumo de energía proporcionada por la IoT, superará en todo el mundo el impacto ambiental de la producción, el despliegue y el mantenimiento de la IoT.

Los **bucles de control ciberfísico** basados en el procesamiento de datos de la IoT en varias escalas de tiempo permiten nuevos niveles de control y prevención. Por ejemplo, al combinar la supervisión avanzada con el aprendizaje automático, el mantenimiento predictivo se puede realizar mucho antes de que surjan problemas y averías en el hardware industrial. Más allá de la mera mejora de los procesos existentes, también se espera que los bucles de control ciberfísico creen procesos y servicios totalmente nuevos, de alto impacto en la sociedad.

Los **componentes robóticos** son el resultado de la implementación de la IoT y contribuyen a ella. Por un lado, los sistemas similares a los robots surgen al combinar sensores y actuadores, e interactuar con bucles de control ciberfísico. Por otro lado, también se despliegan flotas de robots, drones y otros dispositivos autónomos para complementar la infraestructura de la IoT cuando sea necesario; estos dispositivos pueden participar en la adquisiciónrecogida de datos y proporcionar recursos de manera dinámica.

2

Desafíos sociales de la IoT

La IoT ya ha empezado a transformar nuestra sociedad, lo que ha dado lugar a una serie de retos fundamentales de carácter social. Esta sección describe brevemente los desafíos más importantes en este ámbito, así como la manera en que Inria ha contribuido a hacerles frente.

Marco legal: el equilibrio entre la innovación sin permiso y cuestiones éticas

Fiel heredera de la Internet, la IoT afronta un crecimiento extremadamente rápido, impulsada por intereses a veces contradictorios.

Por un lado, la dinámica y las tecnologías del mercado de Internet se han diseñado fundamentalmente para fomentar una innovación rápida y sin permisos. Por otro lado, cada vez surgen más preocupaciones éticas sobre el uso de estas tecnologías, por ejemplo, con respecto a la privacidad o el medio ambiente.

No se puede esperar que los usuarios promedio de la IoT comprendan plenamente las implicaciones del uso que le dan a los productos IoT. Por lo tanto, el desarrollo de marcos legales adecuados es crucial para orientar la IoT.

Sin embargo, la velocidad de adopción suele superar el establecimiento de marcos legales y normativas, creando áreas grises y lagunas. Con la "penetración" prevista de la IoT –en términos de escala, naturaleza y granularidad de los datos recogidos– estas lagunas podrían tener consecuencias nefastas.

Así, se debe actuar con cautela para minimizar este impacto negativo sin que ello suponga un obstáculo para la innovación. En este caso, la capacidad y la responsabilidad recaen fundamentalmente en los gobiernos y los organismos reguladores. En este ámbito, por ejemplo, los beneficios de actuar a nivel de la UE han quedado demostrados por el impacto del Reglamento de Protección de Datos (GDPR).

Confianza ciudadana: Cómo conseguir y retenerla

Para que la adopción de la IoT prospere, se necesita más transparencia, así como el empoderamiento del usuario final con respecto a los gobiernos y la industria.

Capture of ambient noise via cell phones to establish a collaborative map of noise pollution.
© Inria / Photo C. Morel.

Los despliegues de la IoT que reúnen a múltiples partes interesadas suelen estar motivados por intereses que no permanecen alineados a lo largo del tiempo. Sin las herramientas técnicas o jurídicas necesarias, esta desalineación no se puede gestionar de forma justa ni adecuada.

En concreto, comparado con un contexto B2B, los consumidores B2C están más expuestos a estos problemas y pueden requerir un mayor cuidado.

El público está cada vez más al tanto de cómo se utilizan las tecnologías de Internet para la vigilancia masiva impulsada por el Estado (por ejemplo, el escándalo Snowden), para la piratería en línea con fines de lucro o para el capitalismo de vigilancia mediante la personalización avanzada de la publicidad.

En la esfera pública se están produciendo reacciones y críticas contra los planes de despliegues piloto de la IoT más ambiciosos, que podrían fomentar la opacidad

o favorecer los monopolios industriales de facto. Mientras tanto, la confianza de los usuarios se erosiona a medida que estallan las controversias cuando se exponen más fallos de seguridad (¡a menudo bastante básicos!) en innumerables dispositivos de la IoT, y se desvelan más procesos o funcionalidades ocultas que amenazan la privacidad . Es de esperar que haya más controversias: por ejemplo, las posibles compensaciones entre la privacidad y las necesidades de vigilancia de los gobiernos, en un contexto de seguridad nacional.

Una de las principales características de Internet –y podría decirse que uno de sus puntos fuertes hasta ahora– ha sido la confianza en los enfoques que fomentan la autonomía del usuario final para tomar decisiones que no están dictadas por un proveedor o gobierno específico. Sin embargo, las recientes tendencias políticas y técnicas despiertan temores de que el empoderamiento del usuario final y la transparencia estén perdiendo terreno. Un reto crucial para la IoT en este contexto es contribuir a recuperar y conservar estas características y, por tanto, la confianza de los ciudadanos. Obviamente, si la IoT carece de ese potencial, su adopción podría no resultar del modo esperado.

Soberanía

Si no se controla, la IoT podría aumentar la dependencia hacia tecnologías que pueden no ser geopolíticamente neutrales ni compatibles con la privacidad.

A medida que la tecnología desempeña un papel cada vez más central en la vida de las personas, los aspectos de la soberanía adquieren protagonismo, tanto a nivel individual como a nivel estatal.

- Para los individuos, el reto es maximizar y mantener la propia capacidad de liberarse de la dependencia de los proveedores y de la tecnología que podría poner su privacidad en juego. Por ejemplo, para interactuar con sus dispositivos IoT, un usuario soberano podría preferir una configuración a través de una máquina intermediaria controlada completamente por él, frente a las configuraciones que ofrecen una integración más "fluida" con un proveedor de servicios en la nube. Las grandes empresas de "jardín amurallado" podrían desaconsejar algunos enfoques, considerando que el cliente es el atacante que debe ser contenido.
- Para los estados, el reto consiste en minimizar la dependencia de soluciones técnicas que puedan convertirse en armas. Por poner un ejemplo concreto: depender de Linux puede considerarse bastante neutral desde el punto de vista geopolítico, mientras que decidir confiar en Android es una decisión bastante menos neutral, aunque Android esté técnicamente basado en Linux. Tomar

estas decisiones puede ser difícil en áreas que han sido descuidadas durante mucho tiempo (o subcontratadas)

En cualquier caso: nada es gratis. La soberanía conlleva un esfuerzo adicional. Normalmente, para los particulares, esto se traduce en una menor comodidad. En el caso de los estados, las ventajas y desventajas se asemejan a lo que se ve en los entornos empresariales: La soberanía generalmente requiere una inversión significativamente mayor en investigación, desarrollo y mantención. Además, si el deseo de soberanía lleva al desarrollo y uso de más sistemas separados y concurrentes, entonces entran en juego otras cuestiones: por ejemplo, la interoperabilidad. El reto esencial es, por tanto, optimizar esa inversión, para obtener el "mayor rendimiento por cada centavo".

Estandarización

A medida que la tecnología de la IoT se entrelaza más estrechamente con la sociedad y nuestras vidas personales, la creación de normas para la IoT resulta cada vez más importante.

La esencia de la IoT consiste en permitir que sistemas embebidos heterogéneos se conecten e interoperen a través de la red, potencialmente a gran escala. A nadie le sorprende que la normalización ocupe un lugar destacado en el espacio de la IoT, y en particular la normalización de las comunicaciones de red de la IoT. Por ejemplo, las organizaciones de desarrollo de normas (SDO) como el Consorcio de la World Wide Web (W3C), el Grupo de Trabajo de Ingeniería de Internet (IETF) o el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) son lugares destacados donde se toman decisiones técnicas clave que tienen infinitas ramificaciones, incluso a nivel social.

En la práctica, ninguna organización de desarrollo de normas es neutral en cuanto a los valores, y esto se aplica también a la normalización de la IoT. En particular, el poder concentrado de las grandes empresas tecnológicas sobre la sociedad, combinado con su influencia decisiva en la configuración de la próxima norma (o norma de facto) crea situaciones que se deben abordar. Además, es necesario exponer la relación entre las normas tecnológicas de la IoT y los derechos humanos, por ejemplo. El reto aquí es, por tanto, aumentar la conciencia general tanto de cómo funcionan fundamentalmente las tecnologías estándar, y cómo sus características pueden repercutir en los aspectos sociales.

Educación

Cuanto más aproveche la IoT los computadores "invisibles" –como los sensores y actuadores usado inconscientemente–, se torna más necesario que los planes de estudios incluyan los fundamentos de los sistemas ciberfísicos y señalen sus posibles peligros.

La enseñanza de la informática en general es un reto, y más aún sobre la IoT. Esto se debe, en parte, al hecho de que la tecnología de la IoT está todavía muy fragmentada, especialmente en lo que respecta a la IoT de gama baja. Este desafío conlleva varios aspectos:

- *El desarrollo de las habilidades duras necesarias:* a nivel puramente técnico, los problemas de educación se ven obviamente exacerbados en las regiones en las que la educación informática técnica ya está atrasada. Algunas de las habilidades técnicas necesarias para la IoT, como la programación embebida en profundidad, son habilidades demasiado raras.
- *Desarrollar las habilidades blandas necesarias:* en un nivel menos técnico, sigue siendo deseable tener cierto nivel de educación para "sensibilizar", y desarrollar el sentido común y el pensamiento crítico con respecto a lo que los productos de la IoT pueden/deben o no pueden/no deben hacer. Este pensamiento crítico podría estar a punto de convertirse en algo poco común, un cambio potencial para nuestra sociedad.

Desde un punto de vista filosófico, la forma en que percibiremos la realidad en un mundo totalmente habilitado para la IoT es en sí misma un tema de estudio. A través de sensores y actuadores, no sólo la realidad virtual, sino también la realidad física se puede personalizar y experimentar de forma distinta. Por un lado, iniciativas tales como la postfenomemología pretenden caracterizar la interacción entre los seres humanos, el mundo natural y las tecnologías modernas, que cada vez se convierten en mediadores no neutrales. Por otro lado, algunos diseñadores ya trabajan en el diseño de sistemas sociotécnicos: es decir, un diseño que no sólo considera el material digital y tecnológico, sino también a los propios usuarios humanos como material.

Lucha contra el cambio climático y el agotamiento de los recursos

La IoT puede servir como instrumento para combatir el cambio climático, pero la proliferación de aparatos de IoT es también un vector de agotamiento de recursos.

El despliegue de miles de millones de dispositivos de IoT consumirá en todo el mundo grandes cantidades de energía y recursos (incluyendo plásticos, metales y baterías) para producir, transportar y hacer funcionar estos dispositivos. Ante la actual crisis ecológica, hay que analizar la relevancia de estos dispositivos. A priori, la IoT proporciona los componentes y las herramientas clave que se necesitan para hacer un seguimiento preciso en tiempo real tanto del cambio climático como del

Predicción de las heladas en los huertos de duraznos. © Inria / Photo G. Scagnelli.

efecto de las políticas instauradas para frenarlo. Además, la IoT puede facilitar los medios para automatizar los ajustes dinámicos y aplicar las optimizaciones en una amplia variedad de sistemas complejos que consumen muchos recursos y energía, por ejemplo, los flujos de trabajo industriales o los sistemas de gestión de la energía de las viviendas y los edificios inteligentes. Por lo tanto, no hay duda de que la IoT puede servir para luchar contra el cambio climático. Sin embargo, la eficiencia energética y de recursos de la IoT se debe investigar continuamente, y se deben diseñar restricciones legales que guíen esta eficiencia de forma evolutiva.

Contribuciones por parte de Inria para afrontar los retos sociales de la IoT

Como agencia gubernamental que combina una amplia experiencia científica y una importante producción de investigación aplicada en dominios relacionados con la IoT, con impacto en la educación, la soberanía, las normas y los marcos legales, Inria contribuye a ganar la confianza del público con respecto al uso de las nuevas tecnologías de IoT.

Inria contribuye en la práctica a hacer posible la soberanía en el ámbito de la IoT, de múltiples maneras. Inria promueve la **soberanía** mediante la realización de investigaciones científicas catalogadas de excelencia por sus pares y la publicación sistemática de los resultados en espacios de libre acceso. No obstante, más allá de esta implicación desde el punto de vista científico, Inria también contribuye en otros niveles. Los equipos de Inria participan en colaboraciones técnicas internacionales e interdisciplinarias, y supervisan el despliegue de nuevas tecnologías de IoT en diversas aplicaciones del mundo real.

Inria produce, publica y mantiene software de código abierto. Se han creado grandes comunidades de usuarios en torno a varios proyectos de software de código abierto de gran impacto encabezados por Inria (RIOT, Scikit-learn, etc.). Estos bloques de software son plataformas en las que se puede confiar para ofrecer el máximo rendimiento y garantizar la neutralidad geopolítica. Otro ejemplo de las contribuciones de Inria a la **soberanía** en el ámbito de la IoT es la forma en que Inria aplica su experiencia científica a las iniciativas de **estandarización** abierta. Por ello, Inria es coautor habitual de las nuevas especificaciones de estándares abiertos para la IoT, publicadas por organizaciones de desarrollo de estándares de gran impacto, como el IETF y el W3C.

Inria también utiliza su experiencia en diversos ámbitos científicos relacionados con la IoT para contribuir a los debates sobre los marcos legales y las salvaguardas para la IoT. Por ejemplo, las actividades de investigación en Inria incluyen evaluaciones de los problemas prácticos de cumplimiento de la normativa europea GDPR, para los productos de consumo de IoT en el segmento del hogar inteligente.

Inria contribuye activamente a la **educación** en el campo de la IoT, en varios niveles. Muchos investigadores de Inria también imparten clases, en el marco de una cátedra universitaria o equivalente. Sin embargo, Inria también contribuye a la **educación** sin limitarse a esta tradicional participación de los investigadores en la enseñanza. Por ejemplo, Inria ofrece cursos en línea masivos y abiertos

(MOOC) concebidos para un público más amplio en el ámbito de la IoT, seguidos por miles de participantes en todo el mundo. Inria también ha creado programas educativos dirigidos a las categorías de edad más jóvenes, dotando a los jóvenes de 15 años de conocimientos para comprender mejor la tecnología digital. Otro ejemplo destacado de la participación de Inria en actividades educativas es la serie de informes y publicaciones técnicas de Inria, tales como el presente documento.

3

Desafíos científicos y técnicos de la IoT

Lo que esperamos de la IoT va desde empoderar a las personas con servicios revolucionarios hasta tener un gran impacto en la sociedad y la industria, y posiblemente salvar el planeta mediante la lucha global contra el cambio climático.

¿Qué retos científicos hay por delante para hacer realidad tan altas expectativas? A continuación resumimos una lista de preguntas que consideramos clave para la IoT.

¿Cómo preservar la privacidad con la IoT ubicua?

Existe una tensión permanente entre la explotabilidad de los datos de la IoT y la privacidad de sus usuarios. En un extremo, los datos de los usuarios de la IoT deberían poder explotarse masivamente cuando se trata de salvar vidas. En el otro extremo: el despliegue de la IoT ubicua podría servir de base para un "panóptico" electrónico. Este sistema podría aniquilar por completo la privacidad individual. Por lo tanto, una pregunta crucial es: ¿cómo, y hasta qué punto, podemos garantizar una sólida protección de la privacidad al tiempo que conservamos la utilidad de los datos de la IoT?

Un tipo de problema es el diseño de novedosos paradigmas y técnicas de preprocesamiento aplicables directamente en los dispositivos IoT, que ofuscan partes de los datos que no corresponden a un "interés legítimo" específico. Otro tipo de problema es el diseño de primitivas criptográficas novedosas, aplicables incluso en dispositivos IoT de baja potencia, potentes incluso frente a atacantes post-cuánticos.

¿Cómo aumentar la resiliencia, la seguridad y la protección en la IoT?

A medida que dependemos cada vez más de los nuevos servicios construidos sobre la IoT, su resiliencia frente a la interrupción parcial de la infraestructura o el mal funcionamiento del subsistema se vuelve crucial. Los despliegues de IoT implican arquitecturas de sistemas distribuidos progresivamente más complejos, por lo que un diseño orientado a la resiliencia sigue siendo un reto importante. El nivel de fiabilidad también influye en la seguridad de la IoT.

La ciberseguridad solía referirse principalmente al ciberespacio, es decir, mantener segura la información digital, utilizar una buena "netiqueta" (etiqueta de Internet), etc. Sin embargo, con la IoT, la ciberseguridad se extiende del espacio virtual al físico: ahora la ciberseguridad también se refiere a la seguridad de la integridad física y a la protección del entorno en el mundo real.

Mapa de las cosas: recopilación de datos e información para los usuarios de objetos conectados.

© Inria / Photo C. Morel.

¿Cuáles son los nuevos riesgos de seguridad con la IoT? ¿Qué beneficios aportan? Los meros "dispositivos IoT" podrían no justificar los riesgos. Se necesitan nuevos modelos para captar tanto a los atacantes como los aspectos de seguridad, en contextos complejos de IoT. A continuación, a partir de estos modelos, se requieren mecanismos novedosos para ofrecer garantías sobre el software, el hardware y la comunicación de los dispositivos IoT, a lo largo de su vida útil, que puede durar décadas. Este reto se agrava en el caso de los dispositivos IoT de baja potencia, que son el nuevo "eslabón más débil".

¿Cómo aliar el aprendizaje automático con la IoT?

Las aplicaciones que utilizan la inteligencia artificial y el aprendizaje automático (ML, por sus siglas en inglés) se están desarrollando en múltiples ámbitos que crecen a gran velocidad. Desde esta perspectiva, la IoT es, al mismo tiempo, un enorme proveedor de los valiosos datos necesarios para entrenar los modelos

de ML y un consumidor de capacidades de inferencia basadas en estos modelos.

Una cuestión clave es cómo aprovechar muchos más datos de la IoT, con mucha menos presión sobre la privacidad y la demanda de la red. Uno de los desafíos es diseñar alternativas al entrenamiento centralizado de modelos de ML, que distribuyan el entrenamiento, por ejemplo, de forma federada entre pares. ¿Cuán robusto y eficiente puede ser el aprendizaje distribuido? ¿Hasta dónde podemos llevar los requisitos de recursos para un par de aprendizaje? Por otro lado, otro de los retos es cómo habilitar capacidades de inferencia en dispositivos IoT más pequeños, con menos pérdida de rendimiento, al tiempo que se mantiene la flexibilidad de modificar los modelos utilizados en estos dispositivos a posteriori.

¿Cómo ampliar la conectividad de último salto para la IoT?

La IoT depende fundamentalmente de la conectividad de miles de millones de nuevos dispositivos situados en el borde de la red. Para adaptarse al consiguiente aumento del tráfico, se necesitan protocolos de red de nueva generación que hagan frente a la escasez de medios de comunicación y mejoren la capacidad de los segmentos dispositivo-infraestructura y dispositivo-dispositivo.

Con tantos dispositivos, incluidos los de muy bajo consumo, las tecnologías de red de última generación para el último salto deben ser extremadamente asequibles, tanto en términos de gastos de capital como costos de funcionamiento. ¿Cómo podemos fomentar una dinámica similar a la de Internet, en la que "la conectividad es su propia recompensa"? Al mismo tiempo, se espera una mejor penetración en interiores y una menor necesidad de energía, así como una comunicación de mayor alcance en exteriores para llegar a lugares más remotos. Las nociones de "último salto" y "dispositivos IoT" tendrán que ampliarse a lo extraterrestre, como demuestran las actuales carreras orbitales y espaciales.

¿Cómo ampliar los principios de las redes de extremo a extremo para la IoT?

Internet se ha ampliado rápidamente según el principio de que la inteligencia se sitúa en los puntos finales, en lugar de ocultarse dentro de la red. La IoT desafía este principio. ¿Hasta qué punto podemos ampliar los fundamentos de las redes de extremo a extremo?

En la última década, los mecanismos de extremo a extremo, como los protocolos de red 6LoWPAN IPv6 de estándar abierto y los trabajos preliminares sobre la Web de las Cosas (WdC), insinúan lo que podría ser la IoT de extremo a extremo en el futuro. Sin embargo, aún quedan desafíos para completar una arquitectura adecuada para la IoT. Delegar parte de la inteligencia en los servidores proxy parece inevitable para los dispositivos IoT de muy baja potencia; pero, ¿cómo y hasta qué punto? Además, se necesitan nuevos protocolos y semánticas para automatizar niveles adicionales de comunicación entre máquinas.

¿Qué interfaces hombre-máquina requiere y permite la IoT?

Por un lado, la IoT añade miles de millones de nuevas interfaces al mundo físico, desde el ciberespacio. A la inversa, ¿cómo pueden los usuarios humanos de la IoT interactuar de mejor manera con el ciberespacio, a través de estas interfaces?

Es fundamental mejorar tanto la accesibilidad como el control de estas interfaces. Uno de los aspectos es la identificación de los niveles adecuados de control con los que capacitar a los seres humanos. Los seres humanos son una multitud heterogénea, con diferentes capacidades y requisitos para comprender lo que ocurre bajo el capó de la IoT. Otro aspecto es diseñar una ergonomía novedosa que pueda encarnar físicamente algunas partes del ciberespacio. El desafío consiste en ayudar a los usuarios a aprender, comprender y apropiarse de la tecnología de la IoT, incluso cuando esta crece y cambia a lo largo del tiempo.

¿Cómo acortar las distancias entre la IoT, el control y la robótica?

A medida que la IoT interconecta sensores y actuadores con capacidad de cálculo, disponible local o remotamente, a través de la red, aparecen nuevas variedades de bucles de control.

¿Qué bucles se pueden aprovechar? ¿Cómo se debe afinar el control? Por un lado, la investigación en el campo de la IoT industrial tiene como objetivo establecer y optimizar el control sobre cadenas de suministro y producción extremadamente complejas. Los sistemas híbridos distribuidos que mezclan estados continuos y eventos discretos son muy difíciles de modelar y controlar. Por otra parte, los microrrobots y la robótica de enjambre se pueden considerar como una próxima

frontera, ya que exigen abordar simultáneamente muchas cuestiones de investigación abiertas, como la previsibilidad de la latencia, la movilidad, la localización y la resolutividad de los recursos en función de los requisitos de bajo consumo.

¿Cómo habilitar los dispositivos IoT de escala milimétrica?

Los últimos avances en microelectrónica superan los límites de la miniaturización extrema: los prototipos de chips del tamaño de un grano de arroz (o menos) pueden detectar, calcular y comunicarse vía inalámbrica, sin necesidad de componentes adicionales. Este polvo inteligente tiene el potencial de revolucionar los micro-portátiles y la robótica de enjambre, pero presenta desafíos únicos con vistas a interoperar con la comunicación inalámbrica estándar de baja potencia, en términos de programación embebida y calibración.

¿Cómo avanzar hacia reducir a cero la huella de recursos con la IoT?

La IoT puede ser una herramienta para ejecutar políticas medioambientales, o para medir su efecto. No obstante, ¿qué pasa con la huella de recursos de la propia IoT?

Minimizar el costo medioambiental de la producción y el funcionamiento de los dispositivos individuales es clave para disminuir la huella de la IoT y para hacer asequible el despliegue masivo que se necesita. Uno de los aspectos es la producción de dispositivos electrónicos con una cantidad considerablemente menor de materiales no renovables, como el plástico y el metal. Otra es el diseño de nuevos paradigmas de hardware, software y redes embebidas que puedan aprovechar la energía ambiental intermitente y ofrecer soluciones de balance en cuanto a rendimiento y consumo de energía.

La evaluación del impacto global de la IoT sigue siendo un reto. A nivel mundial, ¿cuáles son los beneficios netos y la huella de la IoT? Se requiere un esfuerzo interdisciplinario complejo para captar la imagen global de los impactos directos e indirectos, los ciclos de vida completos y los efectos inducidos.

Contribuciones de Inria para afrontar los retos científicos y técnicos de la IoT

Para abordar las cuestiones científicas identificadas anteriormente, necesitamos la informática en diversos ámbitos, entre ellos:

- *redes de comunicación,*
- *representación de datos,*
- *sistemas distribuidos,*
- *criptología,*
- *procesamiento de datos y privacidad,*
- *seguridad, fiabilidad y certificación,*
- *interacción hombre-máquina,*
- *control,*
- *seguridad,*
- *arquitectura de hardware de bajo consumo, programación y compilación,*
- *optimización de la huella global de recursos.*

Los investigadores de Inria llevan a cabo actividades científicas que contribuyen al avance del estado del arte en cada uno de los campos de investigación de la IoT mencionados anteriormente. En la segunda parte de este documento, analizamos más detenidamente el conjunto de retos de investigación de la IoT dentro de cada uno de estos ámbitos.

PARTE II

Campos de investigación para la IoT

A continuación nos adentramos en diferentes campos de la investigación informática que se deben aprovechar, y que requieren avances, para abordar las cuestiones científicas clave que hemos identificado, relativas a la IoT.

> Los siguientes capítulos (que abarcan amplios campos de investigación) pretenden ser bastante autocontenidos, y se pueden leer en cualquier orden. Por ejemplo, el lector podría optar por leer el capítulo sobre Criptología para la IoT de gama baja antes de leer el capítulo sobre Redes de comunicación para la IoT. Dentro de estos capítulos, el documento no busca abarcar de forma exhaustiva los temas de investigación relacionados, sino que pretende poner de manifiesto la diversidad de problemas en los que se trabaja.

> Los lectores rápidos y los menos interesados en profundizar en la ciencia y la tecnología pueden hojear brevemente los títulos de los siguientes capítulos/secciones y saltarse hasta el final del documento

2.1 Redes de comunicación para la IoT

Tanto el borde de la red como su núcleo prevén un impacto significativo, a medida que la IoT y la comunicación de máquina a máquina (M2M) aumentan

Optimización de los protocolos de acceso a la red IoT

En el borde de la red, la multitud de dispositivos IoT dependeN de una conectividad eficiente y disponible para conectarse a la red. Los estudios ya indican que nos estamos acercando a un estado en el que el 75% de los dispositivos y las conexiones en Internet provienen del segmento de los consumidores. Los protocolos de acceso inalámbrico constituyen un reto especialmente importante.

Los dispositivos IoT de gama alta, cada vez más ávidos de rendimiento, desafiarán inevitablemente a la tecnología inalámbrica de vanguardia. La tecnologías anunciadas de acceso inalámbrico de alta potencia (rango de vatios), tales como el Wi-Fi 6 o el acceso celular 5G, se verá desafiada por las próximas aplicaciones con gran carga de red, como la realidad virtual totalmente inmersiva y mejorada por la IoT, la realidad aumentada o los vehículos autónomos. El diseño de optimizaciones y nuevos protocolos en este espacio supone, pues, una vía de investigación cada vez más prometedora. El reto científico es acercarse al límite de capacidad de transporte del medio inalámbrico (impuesto por las leyes de la física y la teoría de la información), para aprovechar al máximo el espectro de radiofrecuencias disponible. Un reto técnico asociado es el diseño y la producción de nuevos chips dedicados a la comunicación radiofónica optimizada, que requieren enormes inversiones en I+D.

Técnicas como la MIMO masiva resultan prometedoras para afrontar el reto de la densidad, pero requieren una investigación más profunda para alcanzar todo su potencial. También cabe mencionar que las nuevas soluciones algorítmicas se vuelven atractivas a partir de técnicas de aprendizaje automático (por ejemplo, el aprendizaje de refuerzamiento, o el aprendizaje profundo). Por lo tanto, esperamos que el diseño de optimizaciones y nuevos protocolos de acceso para dispositivos IoT de gama alta sea un área de investigación activa y desafiante en el futuro.

↗ En Inria, el equipo-proyecto **MARACAS** combina la teoría de la información con el procesamiento estadístico de señales, la teoría del control, la teoría de juegos y el aprendizaje automático para explorar nuevas tecnologías que optimicen la comunicación en las capas físicas inalámbricas (PHY). Además de las capas PHY inalámbricas, los equipos de proyectos **TRIBE** y **EVA** trabajan en la optimización del acceso múltiple inalámbrico (por ejemplo, el acceso aleatorio moderno), aprovechando también el aprendizaje automático.

Es necesario explorar técnicas de comunicación complementarias y radicalmente diferentes para aliviar la presión sobre el medio de radiofrecuencia. Por lo tanto, esperamos trabajos y retos derivados de las investigaciones sobre paradigmas de comunicación alternativos, como las nanocomunicaciones o las comunicaciones de luz visible (VLC). Estas tecnologías emergentes, en la frontera de la investigación física, merecen ser analizadas y requieren un trabajo pionero.

↗ En Inria, los equipos de proyectos **AGORA** y **FUN** investigan nuevas tecnologías de comunicación de redes de acceso alternativas utilizando comunicaciones de luz visible (VLC). Las comunicaciones RFID y las infraestructuras híbridas, junto con los nuevos servicios que podrían ofrecer.

Ampliación de la cobertura de la red de acceso a la IoT

En comparación con los dispositivos IoT de gama alta, los dispositivos IoT de baja potencia dependen de tecnologías y protocolos diferentes para el acceso a la red. En lugar de apuntar a dispositivos con un rango de vatios de máximo rendimiento, los protocolos de bajo consumo apuntan a un consumo mínimo de energía (rango de milivatios o menos) para dispositivos IoT de bajo a mediano rendimiento. El campo de las tecnologías de radio de baja potencia para redes personales/de área local (PAN/LAN) **aborda un consumo de energía cada vez menor** para distancias de 1 a 100 metros, y pretende ser lo suficientemente frugal como para requerir únicamente la captación de energía del entorno. Por otro lado, el campo de las tecnologías radioeléctricas de red de área amplia y baja potencia (lpWAN) pretende compensar un rendimiento algo menor para distancias mucho más largas (10 km o más) con el mismo bajo consumo de energía.

↗ En Inria, el equipo-proyecto **DIONYSOS** trabaja en el diseño de mecanismos de control de acceso inalámbrico para grandes redes NB-IoT.

Uno de los principales retos es **ampliar la cobertura de la red** a un sinnúmero de dispositivos IoT de bajo costo y baja potencia. Más allá de la cuestión de la gestión eficaz de las redes de acceso atestadas, esta ampliación supone un reto tanto geográfico como ecológico. Desde el punto de vista geográfico, la cobertura debe llegar tanto a los interiores más profundos como a los exteriores más alejados. Desde el punto de vista económico, **la tecnología de acceso a la red deberá mantenerse muy asequible para los dispositivos de bajo costo.**

Sin embargo, una cobertura de un kilómetro es insuficiente para abarcar dispositivos muy remotos (como en el caso de la agricultura inteligente, donde los sensores se pueden desplegar en campos muy amplios y alejados de la infraestructura urbana) o para proporcionar un rendimiento suficiente que cumpla con los requisitos de la implementación. Por ejemplo, en este ámbito, queda por determinar cuál es el rendimiento alcanzable para la conectividad de acceso a la IoT a través de flotas desplegadas de satélites de órbita baja.

Las comunicaciones inalámbricas multisaltos son otra alternativa, que posiblemente aprovechen múltiples tecnologías de radio, pero requieren que se diseñen nuevos protocolos de enrutamiento adaptados a estas aplicaciones y entornos.

↗ En Inria, equipos de proyectos como **AGORA**, **FUN**, **MARACAS** y **TRIBE** investigan la optimización del rendimiento de los despliegues de sensores inalámbricos de baja potencia y los protocolos de enrutamiento y difusión de datos multisalto en este contexto, mediante metodologías que combinan el modelado teórico, la simulación y los experimentos.

Otra vía de investigación en este ámbito consiste en complementar la infraestructura fija con una flota de robots despachados temporalmente, mediante el despliegue de flotas de vehículos aéreos no tripulados (UAV por sus siglas en inglés, drones) o robots terrestres. Estos recursos adicionales se deben desplegar rápidamente, para restablecer la conectividad después de un fallo, para supervisar un evento puntual, para explorar o supervisar una zona desconocida/hostil o simplemente para descargar periódicamente los datos de los dispositivos remotos que se encuentran fuera del alcance. La idea de desplegar aparatos móviles no tripulados, ya sea sobre ruedas o aéreos, resulta cada vez más atractiva a medida que se comercializan dispositivos con mayor maniobrabilidad. Sin embargo, siguen surgiendo retos para que dichos dispositivos sean plenamente autónomos, ya que se ajustan a presupuestos muy limitados en cuanto a energía, computación y capacidad de almacenamiento, mientras se les exige una gran coordinación, una comunicación sólida y que se compartan las tareas.

↗ En Inria, equipos de proyectos como **ACENTAURI**, **FUN** y **DANTE** diseñan algoritmos de autodespliegue para UAV y robots terrestres, con el objetivo de optimizar la colocación de los robots o aumentar su autonomía.

Optimización de protocolos para redes centrales y de borde

En la actualidad, el núcleo de la red tiene que transportar mensualmente datos medidos en exabytes (miles de millones de Bytes). En el futuro, debido al fuerte crecimiento del tráfico de la IoT, de máquina a máquina, **el núcleo de la red tendrá que transportar una demanda de datos mucho mayor.**

Un desafío importante es, por lo tanto, limitar la velocidad de crecimiento del tráfico de la IoT que fluye a través del núcleo de la red. Para ello, un área de investigación activa **explora arquitecturas de protocolo de red alternativas que tienen como objetivo aprovechar mejor el almacenamiento y el procesamiento de datos en la red,** lo más cerca posible del origen de los datos, como la computación de borde y la red centrada en la información.

Una vía de investigación que se relaciona con esto es la latencia. La latencia media entre la detección y la actuación con la red en el bucle puede ser de unos pocos milisegundos. Sin embargo, algunas aplicaciones de IoT en tiempo real (por ejemplo, Internet táctil, telecirugía) requieren una latencia estrictamente inferior a unas decenas de milisegundos. **Lograr los requisitos combinados de latencia ultrabaja, costo y complejidad para las aplicaciones de IoT en tiempo real** es, pues, un reto importante.

↗ En Inria, el equipo-proyecto **DIANA** diseña, implementa y analiza nuevas arquitecturas de red, servicios y protocolos en el contexto de cientos de miles de millones de dispositivos inalámbricos, cuyo objetivo es la transparencia del servicio y un mejor control de los datos del usuario.

Estandarización de las comunicaciones para la IoT

La esencia de la IoT consiste en permitir que sistemas embebidos heterogéneos se conecten e interoperen a través de la red, potencialmente a gran escala. Por lo tanto, no es de extrañar que los organismos de estandarización de las

comunicaciones de red ocupen un lugar destacado en el espacio de la IoT, lo que incluye a las siguientes entidades:

- **IEEE,** que trabaja en protocolos de comunicación físicos y de capa de enlace, en particular el grupo de trabajo IEEE 802.15, que desarrolla los estándares inalámbricos Bluetooth e IEEE 802.15.4;
- **IETF,** que trabaja en los protocolos de comunicación de la capa de red, transporte y aplicación, incluidos muchos grupos de trabajo que desarrollan el protocolo de red 6LoWPAN y la normalización de la seguridad de la comunicación IPv6 para la IoT de baja potencia;
- **W3C,** y en particular el grupo de trabajo de la Web de las Cosas, que desarrolla esquemas de identificadores de recursos web para la interoperabilidad semántica entre proveedores y consumidores de servicios de la IoT.
- **3GPP** es la destacada organización de normalización que desarrolla protocolos para las telecomunicaciones móviles celulares (NB-IoT, 5G, etc.).

↗ En Inria, los equipos de proyectos, que incluyen **EVA**, **PRIVATICS**, **TRIBE** y **WIMMICS**, contribuyen activamente al diseño y la normalización de protocolos y modelos de datos para redes de baja potencia, dentro de organismos de normalización como el IETF y el W3C.

Sin embargo, aparte de IEEE, IETF, W3C y 3GPP, florece un entramado de organismos de normalización que se reorganizan constantemente. Por eso resulta difícil navegar por el cambiante panorama de las normas, **que a veces se solapan y otras veces compiten entre sí.**

El acceso a la red por radio varía entre LoRa, Sigfox, NB-IoT, Bluetooth LE, ZigBee, Dash7, EnOcean, WirelessHART, DECT ULE, UWB, entre otros. El acceso a la red por cable varía entre PLC, KNX, BACnet, CAN, entre otros. Una gran variedad de estándares de comunicación de nivel superior y modelos de datos semánticos son emitidos por una amplia variedad de organismos y alianzas, incluyendo, pero no limitado a: OMA SpecWorks (desarrolla los estándares LWM2M), OPC Unified Architecture (OPC UA), OASIS (desarrolla los estándares MQTT), DotDot (Zigbee Alliance), One Data Model (OneDM), etc

Desgraciadamente, no sólo el panorama, sino también las propias especificaciones de los protocolos de la IoT, resultan a menudo complejas y desafiantes a la hora de garantizar la interoperabilidad y la seguridad reales entre dispositivos de diferentes proveedores. Un conjunto cada vez mayor de **alianzas que desarrollan marcos de interoperabilidad y certificación surgen en varios verticales**, que incluyen (pero no se limitan a) Thread Group, Connected Home over IP

(recientemente renombrado como Matter), Zigbee Alliance, Open Connectivity Foundation (AllJoyn), WiSun, entre otros.

Un reto importante que tenemos por delante es el de consolidar el panorama de los estándares de la tecnología de comunicación de la IoT. Con la llegada de la IoT, es necesario que de un minuto a otro colaboren técnicos de ámbitos y culturas muy diferentes: por ejemplo, ingenieros de hardware embebido frente a la comunidad que desarrolla los protocolos y el software de Internet. Estas comunidades suelen tener problemas para hablar entre ellas, lo que indica una falta básica de terminología común.

Incluso dentro de cada dominio técnico, la heterogeneidad excesiva es una dura realidad a la que hay que hacer frente en el ámbito de la IoT, a diferentes niveles, incluyendo el hardware, el software, los protocolos de red y los estándares tecnológicos. Las tecnologías de estos campos tienen que converger hacia un puñado de normas (algunas de facto) sobre las que se desarrollará un "punto ideal" que favorezca un progreso más rápido y una interoperabilidad a gran escala, al tiempo que se evitan los escollos de la "monocultura". En pocas palabras: la consolidación del mercado aún no se ha producido en lo que respecta a las tecnologías de la IoT.

Protocolos de red de bajo consumo de extremo a extremo

Han aparecido stacks o conjuntos de protocolos de interconexión de bajo consumo y de uso general. El mejor ejemplo es probablemente el stack de protocolos IPv6 basado en 6LoWPAN y CoAP, estandarizado por el IETF. Sin embargo, en la práctica, aún prevalece un fastidioso desajuste de los protocolos a distintos niveles. Un desajuste típico es el de IPv6, que a menudo no se admite de forma nativa en el borde de la red, que sólo admite IPv4. Otro desajuste típico aparece a menudo entre los proveedores de la nube y los vendedores de dispositivos: estos últimos hablan CoAP sobre UDP por encima de la capa de transporte, mientras que los primeros sólo hablan HTTP sobre TCP. Otro desajuste es la codificación/modelo de datos que se utiliza: la semántica de los datos agregados a partir de diferentes dispositivos IoT no suele coincidir.

Existen soluciones (por ejemplo, para el desajuste anterior, túnel IPv6 en IPv4, o proxy CoAP-HTTP, traducción de codificación de datos). Sin embargo, este desajuste es una barrera de entrada que sigue siendo importante (si no fatal) para la mayoría de los no especialistas. Por tanto, la eliminación de estas barreras sigue

suponiendo un reto. La eliminación de estas barreras no sólo reducirá significativamente el costo de entrada a la IoT, sino que también allanará el camino para que se estandaricen los paradigmas avanzados de almacenamiento y computación en la red para la IoT, que son necesarios para realizar la computación de borde, y para aliviar la carga de la red central.

Independientemente de las soluciones (proxies, pasarelas, entre otros), el reto de los nuevos estándares de protocolo de red de bajo consumo es la adopción generalizada de extremo a extremo, a lo largo de todo el espectro de la nube. En particular, dado que los dispositivos IoT de baja potencia están extremadamente limitados en términos de recursos, las soluciones de extremo a extremo no pueden limitarse a "añadir otra capa de protocolo sobre el legado". La integración de estándares de protocolos de red de bajo consumo es un tema crucial.

Por lo tanto, una cuestión clave es la siguiente: ¿hasta dónde puede llegar el principio de la red de extremo a extremo para que abarque los dispositivos IoT de bajo consumo?

2.2 Representación de datos para la IoT

A medida que conectamos más y más objetos a Internet, éstos se tornan visibles para diversas aplicaciones que se ejecutan en la red, pero en su conjunto, producen datos de IoT en bruto que no suelen ser fáciles de explotar en masa. Los dispositivos heterogéneos de la IoT ("cosas") suelen utilizar diferentes esquemas de representación de datos, y la semántica varía. Esta realidad fragmenta aún más la IoT, en la capa de aplicación. Se necesitan nuevos enfoques que permitan a los desarrolladores crear aplicaciones que abarquen una variedad dispar de objetos y tecnologías: para vincular los objetos con otras partes del sistema, se necesita un marco unificado.

Una propuesta destacada en este espacio es la Web de las Cosas (WdC), que consiste en apoyarse en la Web como plataforma de aplicación universal para los objetos conectados, imaginando literalmente una **Web de todo, y que funcione sobre cualquier cosa.** Esta oportunidad viene acompañada del reto de hacer evolucionar las técnicas clásicas de la Web para abordar el tamaño, la heterogeneidad y las especificidades de los dispositivos y las redes de la IoT.

Por ejemplo, entre los conceptos clave aportados por la Web se encuentran las URI para identificar dispositivos, servicios y actores, que proporcionan el mecanismo de desreferenciación por defecto para obtener descripciones ricas para los identificadores recién descubiertos. Para hacer realidad la web de las cosas, se necesitan nuevos niveles de flexibilidad de los modelos estándar basados en la web que atiendan a:

- los proveedores, para describir las características de sus productos y servicios;
- los proveedores de plataformas y aplicaciones, para exponer estas características;
- los usuarios, para expresar sus objetivos y peticiones, etc.

La flexibilidad de la descripción también es vital para que los fabricantes puedan diferenciar sus productos de los de la competencia y ofrecer una gama de modelos con diferentes características, al tiempo que se mantenga la interoperabilidad por toda la web. Estos modelos genéricos deben hacer valer un estándar compartido cuando corresponda (por ejemplo, tipos de datos básicos, unidades físicas) y proporcionar representaciones neutrales del lenguaje de programación que soporten la interoperabilidad entre plataformas y dominios. Sin embargo,

también deben admitir extensiones para los modelos específicos de la aplicación y el dominio, por ejemplo, un tipado más avanzado y definiciones para estructuras de datos más complejas dedicadas a usos y escenarios específicos.

Aprendizaje automático distribuido para que las aplicaciones de la IoT impulsen la creación y evolución de redes complejas. © Inria / Photo L. Jacq.

Los lenguajes de la Web, y en particular los de los **Datos Vinculados y la Web Semántica,** pueden proporcionar interoperabilidad a niveles superiores y formatos estándar para las descripciones de objetos, operaciones, entradas, salidas, etc. La necesidad de descripción en la WdC es un caso especial de una cuestión abierta en el ámbito de la Web Semántica: ¿cómo formalizar vocabularios multiplataforma y multidominio? El reto es proporcionar lenguajes y vocabularios que cuenten con la expresividad adecuada para representar formalmente la red de "gemelos digitales" de las cosas. En la WdC, las cosas se ven como recursos de software identificados en la Web con características, operaciones y eventos que deben describirse y vincularse para apoyar el descubrimiento, la interoperabilidad y la composición. Los modelos a diseñar no sólo deben ser capaces de describir Cosas muy heterogéneas (sus necesidades, capacidades y características) sino también la plataforma y el contexto ciberfísico.

Al tener que representar, publicar, consultar, validar e inferir a partir de estos metadatos y los datos intercambiados en la WdC, tenemos que diseñar y estandarizar modelos abstractos, sintaxis concretas y serializaciones eficientes, lenguajes de procesamiento aplicables en un contexto dinámico y de recursos limitados, entre otras cosas. Los enfoques clásicos de los datos enlazados en la

web semántica pueden aportar soluciones (por ejemplo, los lenguajes ontológicos), pero también se enfrentan a retos específicos derivados de la web de las cosas. Un reto importante para los modelos de la Web semántica es la capacidad de hacer frente al dinamismo de la WdC, incluidos los flujos de datos (por ejemplo, la salida de los sensores) y la reconfiguración veloz a medida que las cosas se conectan o se eliminan. Otro reto es la necesidad de captar y adaptarse al contexto de la aplicación en términos de alcance, distribución, limitaciones, privacidad, perfiles de usuario, etc. Los modelos de datos estándar también deben admitir la provisión de lenguajes de scripting basados en la web para la interacción Cosa-a-Cosa, las aplicaciones y la gestión, independientemente de la plataforma. Los lenguajes de consulta y validación de datos enlazados se pueden utilizar para acceder a las descripciones y validarlas con respecto a las restricciones. Las representaciones y el razonamiento basados en ontologías pueden apoyar la componibilidad y la interoperabilidad con lenguajes y transformaciones pivote. Los lenguajes pivote y los mecanismos de transformación proporcionados por la web semántica también pueden apoyar la captura y la mitigación de las diferencias entre los protocolos disponibles (por ejemplo, HTTP, WebSockets, CoAP, MQTT) con el fin de proporcionar medios uniformes para enviar y recibir mensajes a las cosas y los servicios, como los enlaces declarativos.

Los esquemas de seguridad también se pueden expresar e intercambiar entre sistemas heterogéneos.

↗ En Inria, el equipo-proyecto **WIMMICS** trabaja en la integración de agentes autónomos en la Web de las Cosas (WdC), apoyándose en los lenguajes de la Web Semántica y en los principios de los datos enlazados para tender un puente entre la arquitectura de la Web y el estilo de la arquitectura multiagente. El objetivo es proporcionar un entorno estándar abierto que permita desplegar agentes y comportamientos inteligentes en los sistemas de IoT, por ejemplo, en contextos tales como la automatización en fábricas.

2.3 Sistemas distribuidos para el continuo Nube-Borde-Cosa

Diseñar, desarrollar y ejecutar aplicaciones en la IoT requiere dominar y gestionar su complejidad en términos de distribución, heterogeneidad, dinamismo y escala.

Middleware para la IoT

Tradicionalmente, el middleware o software intermedio se encarga de gestionar estas cuestiones, de forma transparente para los sistemas distribuidos, ya sea en forma de una capa de software que opera en cada dispositivo, o de una entidad de software en algún lugar de la red que actúe como intermediario. Sin embargo, el diseño de middleware se enfrenta a nuevos retos únicos cuando se trata de dar soporte a espacios y aplicaciones inteligentes en la IoT.

El principal reto es hacer frente al alto nivel de incertidumbre que caracteriza el entorno de ejecución de la IoT, que contrasta con el proceso típico de ingeniería de software, en el que un sistema se finaliza durante su fase de diseño. El contexto de la IoT está en un cambio constante, y la complejidad de los cambios (a los que se debe adaptar el sistema de IoT) es tal que no se puede abordar a la hora de diseñar el sistema. Debido a su composición y ejecución automatizada, dinámica y dependiente del entorno, los sistemas de la IoT surgen de formas no anticipadas. Tanto los sistemas como sus propiedades adquieren su forma completa sólo durante la ejecución y suelen evolucionar a posteriori, lo que requiere niveles no previstos de interoperabilidad.

Una aplicación destacada del middleware de la IoT es el "crowdsensing" o la detección masiva y participativa, por ejemplo, para la vigilancia del medioambiente urbano. Un reto asociado al middleware de la IoT es el diseño de nuevos algoritmos y protocolos capaces de integrar eficazmente la adopción masiva de teléfonos inteligentes y otros dispositivos de IoT controlados por el usuario, y de gestionar la participación dinámica y a gran escala de los usuarios IoT. Además de la detección física, en la que el sensor de un dispositivo informa pasivamente de los fenómenos detectados, entra en juego la detección social, en la que el usuario es consciente y participa en la detección del entorno.

Otro reto asociado se deriva de la baja precisión de los sensores y de las condiciones no controladas en la detección participativa. Resulta especialmente difícil lograr que el crowdsensing oportunista se convierta en un medio fiable de observación de los fenómenos medioambientales. Un campo de investigación es el diseño de esquemas de coordinación espontánea y descentralizada entre sensores móviles.

↗ En Inria, los equipos de proyectos, como **MIMOVe** y **SPIRALS**, trabajan en soluciones de middleware que dan soporte a espacios y aplicaciones inteligentes en el IoT. Por ejemplo, DeXMS es un middleware desarrollado por Inria con el objetivo de proporcionar interoperabilidad, composición y programación de sistemas dinámicos para los sistemas emergentes de la IoT, al tiempo que depende de los recursos computacionales en el borde de la red. Otras plataformas de middleware desarrolladas por Inria, como APISENSE o SenseTogether, tienen como objetivo el crowdsensing móvil. El objetivo de este middleware es mejorar la calidad de los datos de la IoT y aprovechar el conocimiento del contexto, así como los recursos de borde, incluidos los propios sensores de crowdsensing móviles.

Plataformas de testeo para el continuo Nube-Borde-Cosa

La IoT aporta miles de millones de aparatos conectados con poca capacidad de computación. Estos aparatos pueden colaborar en la red. La colaboración puede darse entre dispositivos IoT, o con algunas máquinas cercanas que proporcionen capacidades de computación medianas (también conocidas como computación "edge" o borde, o "fog-computing") o con máquinas más remotas que proporcionen una gran capacidad de computación (cloud-computing o computación en la nube). Así, surge un espectro continuo Nube-Borde/Fog-Cosa, a lo largo del cual se puede distribuir adecuadamente la computación, en función de los requisitos de alto nivel (que pueden evolucionar con el tiempo).

↗ Inria lidera el desarrollo de grandes infraestructuras de prueba para la investigación experimental en el continuo Nube-Borde-Cosa. Por ejemplo, Inria desarrolla **SILECS**, una plataforma de pruebas de acceso abierto que permite a los investigadores generar y desplegar el stack completo, el software y los protocolos, de extremo a extremo, desde pequeños objetos conectados hasta grandes centros de datos. El objetivo es capturar de forma integral y detallada los eventos, desde los sensores/actuadores hasta el procesamiento y almacenamiento de datos, las transmisiones de radio y el despliegue dinámico de los servicios informáticos de borde.

Orquestación de recursos Nube/Borde/Fog/Cosas

Los diseñadores de sistemas ciberfísicos tienen la tarea de programar el espectro Nube-Borde/Fog-Cosa. Más concretamente, hasta ahora se han utilizado técnicas y paradigmas muy diferentes para programar y gestionar estas distintas categorías de máquinas (nube, borde, cosa). Por ello, es difícil comprender y evaluar el sistema en su conjunto. Por lo tanto, la orquestación dinámica de los recursos Nube-Borde/Fog-Cosa sigue suponiendo un desafío. Otros desafíos derivados incluyen evaluaciones integrales de las características globales de seguridad y privacidad de los sistemas ciberfísicos. Una línea de investigación en este campo sería el diseño de una sintaxis unificadora para programar todos los componentes del sistema ciberfísico, lo que permitiría una caracterización ciberfísica global. Este enfoque pretende abordar y aplicar la seguridad a lo largo del continuo, (en lugar de abordar la seguridad componente por componente) y simplificar el comportamiento temporal no trivial de la programación de la IoT mezclando actividades síncronas y asíncronas.

↗ En Inria, el equipo-proyecto **INDES** trabaja en el diseño de lenguajes de programación seguros y multi-capasde varios niveles para la IoT, con una sintaxis que abarca todo el proceso, desde los microcontroladores hasta la nube. Por ejemplo, **INDES** desarrolla Hop.js y HipHop.js. Con estos dialectos de JavaScript, los servidores, los clientes y los dispositivos IoT se programan con el mismo código, lo que simplifica el diseño del sistema IoT y permite reforzar la seguridad a nivel global

DevOps para sistemas ciberfísicos

Se necesitan cadenas de herramientas para reducir el tiempo que transcurre entre la realización de un cambio en un sistema (grande y distribuido) y su despliegue en producción, al tiempo que se garantice una calidad óptima. DevOps es un campo tanto técnico como de investigación que utiliza y desarrolla este tipo de cadenas de herramientas, para el software, abarcando todas las etapas de codificación, construcción, pruebas, empaquetado, liberación, configuración y supervisión durante la vida útil del sistema. En la práctica, el DevOps se necesita para permitir el desarrollo y el mantenimiento ágil que se espera del software moderno en la era de Internet. Las cadenas de herramientas tradicionales no suelen ser aplicables a los dispositivos IoT más pequeños, debido a las limitaciones derivadas de las redes de baja potencia y los recursos integrados. Con los sistemas ciberfísicos que abarcan todo el espectro (Nube-Borde/Fog-Cosas), uno de los

retos es el diseño y la implementación de cadenas de herramientas novedosas y completas, que amplíen el soporte a dispositivos IoT más pequeños y de bajo consumo. Un reto que está naturalmente asociado es el de evaluar y garantizar las propiedades de seguridad de estas cadenas de herramientas extendidas.

Corrección de errores en objetos IoT operados de forma remota con Pharo. © *Inria / Photo Raphaël de Bengy.*

↗ En Inria, el equipo-proyecto **TRIBE** trabaja en el diseño de enfoques DevOps seguros que puedan extenderse a dispositivos IoT de muy bajo consumo, aplicables no sólo a máquinas que utilizan microprocesadores, sino también a máquinas que utilizan microcontroladores conectados más pequeños.

Colocación óptima de la computación en la IoT post-nube

El procesamiento de los datos de la IoT en la nube se puede complementar (o evitar por completo) utilizando la potencia de cálculo más cercana al origen de los datos en bruto de la IoT. No sólo los dispositivos intermedios de borde/fog pueden aportar potencia de cálculo, sino también, en cierta medida, los propios dispositivos IoT de gama baja. La IoT post-nube ofrece potencialmente capacidades de preprocesamiento de datos en cualquier lugar de la red, de extremo a extremo. Con esta posibilidad, surge el reto de identificar y aplicar estrategias para la colocación óptima de los servicios de IoT, el cálculo de datos o el preprocesamiento,

a lo largo del continuo (nube/borde/fog/cosas). Uno de los retos asociados es la automatización de la migración de servicios a lo largo del espectro, para adaptar dinámicamente el sistema ciberfísico a la evolución de los requisitos de alto nivel. Por ejemplo, algunas comunidades de investigación tales como COIN están explorando arquitecturas de red alternativas definidas por software y centradas en los datos, así como la virtualización de las funciones de red (NFV), que podrían contribuir a abordar este reto.

↗ En Inria, el equipo-proyecto **STACK** trabaja en el diseño de mecanismos de sistemas y abstracciones de software para gestionar y utilizar las próximas generaciones de infraestructuras de Computación Utilitaria, combinando la Nube, Niebla (Fog), el Borde y más allá. Dichas técnicas tienen como objetivo gestionar de forma eficiente el ciclo de vida de las aplicaciones que se ejecutan en el continuo Cloud-IoT, y tienen en cuenta los costos como el consumo de energía, el requisito de retraso de las aplicaciones, las limitaciones de ancho de banda y la seguridad como dimensiones transversales.

Surgen nuevas arquitecturas de acceso inalámbrico que promueven una mayor "softwarización" de la infraestructura de red (un ejemplo destacado es la telefonía móvil 5G y demás). La tendencia es cambiar el costoso hardware de punto de acceso (propietario) por antenas "sencillas" emparejadas con software backend que se ejecuta en servidores genéricos baratos en la nube (o en el borde). Estas redes definidas por software (SDN) aumentan considerablemente la flexibilidad de la infraestructura de acceso inalámbrico y pueden alterar los modelos de negocio de los proveedores y operadores. Estas arquitecturas pueden dar cabida no sólo a una "fragmentación" más avanzada de los recursos de acceso a la red, sino también a nuevas capacidades informáticas específicas de los usuarios, de forma dinámica. Surgen nuevas compensaciones en términos de costo, latencia, fiabilidad, etc.

Un aspecto relacionado es la movilidad de los usuarios de IoT, que crea tanto retos como oportunidades. Al explotar los patrones espacio-temporales de la movilidad de los usuarios, el sistema podría proporcionar una base para estrategias de asignación de recursos más precisas y ágiles. Los retos en este ámbito incluyen, por un lado, la caracterización (y predicción) de la movilidad de los usuarios de IoT y, por otro, el diseño de esquemas dinámicos de descarga y colocación de la computación que puedan aprovechar estos patrones.

↗ En Inria, el equipo-proyecto **TRIBE** trabaja en el diseño de nuevas estrategias de descarga y colocación de la computación para la IoT aprovechando la movilidad de los usuarios, y en la evaluación del impacto de la descarga de tareas a la computación de borde, en el consumo de energía y la latencia en contextos de IoT móvil.

Capacidad de mantenimiento del software IoT distribuido

Aunque los despliegues de IoT se multiplican en una amplia variedad de sectores verticales, demasiados dispositivos IoT carecen de un mecanismo de actualización de software seguro incorporado. Otros pueden tener mecanismos de actualización de software incorporados, pero no se utilizan por razones no técnicas, como la falta de incentivos para el proveedor (o que éste haya quebrado). Sin embargo, sin la disponibilidad (y el uso) de estos mecanismos, las vulnerabilidades críticas de seguridad no se solucionan, y los dispositivos de la IoT se convierten en una responsabilidad permanente, como han demostrado los recientes ataques a gran escala. De hecho, un gran número de dispositivos IoT desplegados que han estado funcionando de forma autónoma durante años (o décadas) ejecutan un software sin mantenimiento. Por ejemplo, muchos elementos de la red de bots Mirai IoT (así como otros objetivos potenciales de esta red de bots) siguen funcionando sin parches al día de hoy, a pesar de que Mirai se descubrió hace varios años y de que se han desarrollado parches desde entonces, ¡y eso a pesar de que estas máquinas disponen de relativamente muchos más recursos que los dispositivos IoT de baja potencia!

Desde el punto de vista jurídico, en lo que respecta a las actualizaciones de seguridad, las cuestiones asociadas se refieren al deber de diligencia: ¿qué impone el deber de diligencia para la IoT que se va a desplegar? ¿Qué impone para la IoT ya implantada (legada)?

Desde el punto de vista técnico, un reto importante es habilitar y automatizar las actualizaciones legítimas del software de seguridad para los dispositivos IoT. Por un lado, la imposición de la legitimidad de las actualizaciones de software también puede conducir a la llamada computación traicionera, que paradójicamente puede impedir las actualizaciones de software necesarias. Por otro lado, en los dispositivos IoT de baja potencia, el reto se ve agravado en primer lugar por las estrictas limitaciones de recursos en términos de rendimiento de la red, energía y presupuesto de memoria.

Las investigaciones anteriores en este campo se han centrado sobre todo en casos de uso sencillos en los que las actualizaciones apuntan a un software de un solo archivo binario, o un software de un único proveedor. Sin embargo, a medida que el software de la IoT evoluciona y se complejiza, esta simplificación deja de ser válida: cada vez más, el software de la IoT se asemeja al de Internet en el sentido de que se convierte en un mosaico de componentes desarrollados, mantenidos y actualizados por diferentes partes interesadas. Hoy en día, en una empresa promedio, menos del 5% del software que se utiliza es de producción propia, mientras que más del 95% es de terceros o de código abierto.

Por lo tanto, un desafío abierto es cómo asegurar de forma eficaz el software de múltiples partes interesadas en dispositivos IoT de gama baja, en los que las partes interesadas tienen una confianza mutua limitada. Hay varios aspectos que entran en juego, que deben combinar la producción de los dominios de investigación, entre ellos:

- mecanismos novedosos de sistemas embebidos profundos para alojar y poner a prueba diferentes componentes de software,
- habilitar y asegurar la cadena de suministro de software de IoT,
- mecanismos eficientes de red de IoT de bajo consumo que transporten actualizaciones modulares.

En la práctica, la mantenibilidad también implica la capacidad de supervisar y gestionar los dispositivos IoT durante su funcionamiento, de forma remota, a través de la red. Por ello, un campo de investigación actual es el desarrollo de protocolos de bajo consumo y modelos de datos de gestión adecuados para los dispositivos IoT conectados mediante señales de radio de bajo consumo. Un área de investigación asociada es la instrumentación eficiente de los dispositivos IoT con fragmentos de código de depuración/monitorización a bajo nivel, insertados y eliminados bajo demanda durante su ejecución, de forma remota, a través de la red de bajo consumo. También se debe seguir investigando sobre el software adaptativo, para pasar de un software meramente adaptativo a un software autoadaptativo. De hecho, la automatización avanzada podría permitir que el software se autorregule.

↗ En Inria, el equipo-proyecto **SPIRALS** trabaja en sistemas autoadaptativos, con el objetivo de introducir más automatización en los mecanismos de adaptación de los sistemas de software, centrándose principalmente en las propiedades de autocuración y autooptimización.

Por último, pero no menos importante, la capacidad de mantenimiento de los dispositivos IoT depende en gran medida de la coevolución del hardware y el software de bajo nivel. Por ejemplo, desde el punto de vista del mantenimiento, se prefiere una implementación de software de una función criptográfica (que se puede modificar fácilmente más adelante para corregir errores o aplicar una nueva normativa). Por lo tanto, los retos de investigación sobre la mantenibilidad incluyen la mejora del rendimiento de las implementaciones de software de funcionalidades críticas de los sistemas embebidos de bajo nivel y el diseño de aceleradores de hardware que perduren en el tiempo (genéricos).

UNA NOTA SOBRE LOS MODELOS DE NEGOCIO.

La mayoría de los modelos de negocio hasta ahora se centran en ganar dinero mediante el despliegue o la explotación de la IoT. Hay menos conocimiento sobre las utilidades que se generan a través del mantenimiento de la IoT, y que sin embargo es clave.

Una vez que los productos IoT se han desplegado y puesto en marcha, es necesario habilitar relaciones menos feudales entre los usuarios finales de la IoT y los proveedores. En concreto, es necesario que las actualizaciones del software de los productos de IoT sean más fáciles en general, incluso en los casos en que el fabricante original no las suministre (ya sea porque fue comprado, quebró o intentó un retiro forzado del producto, por ejemplo). Más allá de las barreras técnicas, las jurídicas (por ejemplo, el incumplimiento de un contrato o una garantía) suelen dificultar, o incluso imposibilitar, las actualizaciones de software. Esto imita un modelo de "jardín amurallado", que permite a los usuarios añadir sólo componentes de hardware autorizados, o comprar sólo servicios de reparación de distribuidores autorizados.

Por ejemplo, los proveedores de IoT que deben certificar sus productos de IoT en cuanto a seguridad actualizan el software de estos productos con escasa frecuencia. Por otro lado, los usuarios podrían querer actualizar el software más a menudo, por ejemplo, para obtener funcionalidades. Hay informes que muestran cómo estas tensiones ya han producido situaciones desafortunadas en las que los usuarios recurren a software IoT pirateado (¡!), lo que no hace más que complicar las cosas.

2.4 Criptología para la IoT de baja gama

La criptografía proporciona protocolos fundamentales y algoritmos básicos ("primitivas") para la autenticación, la identificación y el cifrado sobre los que se construyen todos los sistemas seguros.

Los criptógrafos tienen décadas de experiencia en el diseño y análisis de criptosistemas y protocolos eficientes para dispositivos relativamente potentes (como computadoras, servidores o teléfonos inteligentes), por un lado, y para dispositivos más limitados, como las tarjetas inteligentes, por otro. El auge de la IoT, con dispositivos ubicuos e interconectados de baja potencia, supone un nuevo y fascinante reto para los criptógrafos, ya que mezcla los requisitos de aplicación del paradigma del PC con las duras limitaciones físicas de los dispositivos de gama baja. En pocas palabras, sabemos cómo dotar de cierta seguridad a los microcontroladores de las tarjetas inteligentes, pero las tarjetas inteligentes nunca fueron concebidas para estar conectadas a Internet; y sabemos cómo dotar de seguridad en Internet a los procesadores potentes, pero no con un presupuesto estricto de bajo consumo. El reto para los criptógrafos es desarrollar primitivas criptográficas de gran potencia que funcionen dentro de las limitaciones y requisitos especiales del paradigma de la IoT.

Primitivas criptográficas para la seguridad de las comunicaciones en la IoT

Las primitivas criptográficas de alto rendimiento y alta seguridad están ahora estandarizadas y ampliamente desplegadas en suites de protocolos como TLS (Transport Layer Security) para la comunicación segura en Internet. Sin embargo, estos algoritmos se han desarrollado y optimizado tradicionalmente para plataformas de mayor potencia: desde servidores y PC, hasta smartphones. Cuando pasamos a dispositivos IoT de gama baja más limitados, las restricciones de recursos se estrechan hasta el punto de que las primitivas convencionales suelen ser demasiado costosas para el dispositivo en cuestión. Por lo tanto, uno de los desafíos más importantes es el desarrollo, la optimización y la adopción de primitivas criptográficas alternativas que proporcionen bloques de construcción

adecuados para las comunicaciones seguras y de bajo consumo de la IoT.

Primitivas criptográficas simétricas y asimétricas

Las primitivas criptográficas se dividen en dos clases fundamentales, simétricas y asimétricas, según su función y aplicación. El cifrado y la autenticación de datos, por ejemplo, son primitivas simétricas; el intercambio de claves y las firmas son primitivas asimétricas. Por lo general, las primitivas simétricas tienen un rendimiento mucho mayor y un menor consumo de recursos. Por otro lado, las primitivas asimétricas ofrecen funcionalidades esenciales (como las firmas digitales) que la criptografía simétrica es literalmente incapaz de proporcionar. Sin embargo, las primitivas asimétricas tienen un costo inevitable ya que necesitan claves comparativamente mayores, estados internos más grandes y cálculos más intensos, lo que supone un mayor consumo de tiempo, memoria y batería. Tanto la criptografía simétrica como la asimétrica optimizadas son necesarias para la comunicación segura de la IoT en la práctica.

Primitivas criptográficas pre y postcuánticas

Con el auge de la computación cuántica, cabe hacer una segunda distinción importante, entre las primitivas pre y postcuánticas. Esta distinción representa un cambio en el modelo de ataque: si un criptosistema está diseñado para resistir los ataques de adversarios equipados tanto con computadores cuánticos como convencionales, entonces se denomina postcuántico. El desarrollo de computadores cuánticos lo suficientemente potentes como para atacar los criptosistemas modernos supone un importante escollo para los físicos e ingenieros. Aunque sólo podemos especular sobre cuándo tendrán éxito, o si lo tendrán, debemos preparar la IoT para un futuro cuántico sea como sea; después de todo, no podemos basar la seguridad del futuro en las carencias de la ciencia.

Criptografía simétrica optimizada para la IoT

Las primitivas simétricas requieren una clave secreta compartida entre las partes que se comunican. Algunos ejemplos importantes son los algoritmos de encriptación de datos, como ChaCha20 y AES (el NIST, y la norma internacional de facto), y la autenticación de mensajes, como HMAC y Poly1305. Las funciones hash (como SHA-3), aunque no suelen tener clave, también se incluyen en la familia simétrica.

Si miramos los dispositivos IoT de gama baja, entramos en el mundo de la criptografía ligera. La criptografía ligera tiene como objetivo proporcionar primitivas

simétricas eficientes con huellas de recursos extremadamente pequeñas, aunque a menudo con niveles de seguridad sustancialmente más bajos. La criptografía ligera es interesante para la IoT por dos razones: en primer lugar, porque permite realizar operaciones criptográficas en dispositivos extremadamente limitados y, en segundo lugar, porque es necesaria para la comunicación de dispositivos de gama baja. El NIST (el influyente organismo de normalización estadounidense) está llevando a cabo un concurso de estandarización para primitivas ligeras candidatas; el resultado de esta competencia tendrá un impacto importante en la criptografía simétrica en el espacio de la IoT.

Cuando se diseña criptografía para dispositivos IoT de gama baja, uno de los desafíos es evitar la "doble penalización" que sufren los microcontroladores en comparación con el espacio de los PCs y smartphones: no sólo las CPUs son más débiles y lentas (penalización de rendimiento 1), sino que además pueden faltar los aceleradores de hardware, lo que obliga a adoptar enfoques exclusivamente de software (penalización de rendimiento 2). Por ejemplo, algunos microcontroladores carecen del soporte de hardware para AES (el estándar del NIST) que se da por sentado en el mundo del PC. En lugar de implementar AES en el software para imitar el mundo del PC, se deberían diseñar y utilizar primitivas criptográficas simétricas alternativas en los dispositivos IoT de gama baja. La experiencia ha demostrado, por ejemplo, que el cambio de AES a un esquema de cifrado centrado en el software, como ChaCha20 , puede suponer una mejora del 30% en el rendimiento de algunas aplicaciones.

↗ En Inria, el equipo-proyecto **COSMIQ** trabaja en el diseño y análisis de primitivas simétricas ligeras. Los investigadores de **COSMIQ** participan en la presentación de propuestas al proceso de normalización de la criptografía ligera que lleva a cabo el NIST.

Scuba: una cadena de herramientas para la seguridad de los objetos conectados. © Inria / Photo D. Betzinger.

Criptografía simétrica para la IoT postcuántica

La criptografía simétrica postcuántica se ha estudiado principalmente en respuesta a amenazas como el algoritmo de Grover, que (muy) aproximadamente nos permite buscar espacios de claves en un tiempo proporcional a la raíz cuadrada del número de claves (mientras que los computadores convencionales requieren un tiempo linealmente proporcional al número de claves). Lo que se dice habitualmente es que para garantizar la seguridad postcuántica de muchas primitivas criptográficas simétricas elementales es cuestión de duplicar la longitud de las claves. El tema, desde luego, tiene muchos más matices, especialmente cuando se consideran sistemas y operaciones simétricas más complicadas. Se está investigando activamente la posibilidad de determinar la verdadera seguridad postcuántica de las primitivas simétricas existentes. No obstante, aunque baste con la simple solución de duplicar la longitud de las claves, esto tendrá un impacto importante en la seguridad de la IoT: además de duplicar el espacio necesario para las claves, el rendimiento y el consumo de recursos de los algoritmos se degradará por factores variables. Por ejemplo, pasar de la primitiva criptográfica SHAKE128 a la primitiva correspondiente con longitud de clave duplicada (SHAKE256) no tendrá ningún impacto en los requisitos de memoria, pero podría imponer al menos una disminución del 20 % en el rendimiento.

↗ En Inria, el equipo-proyecto **COSMIQ** trabaja en la seguridad de los criptosistemas simétricos postcuánticos.

Criptografía asimétrica optimizada para la IoT

A diferencia de las primitivas simétricas, las asimétricas dependen de que cada parte mantenga un secreto privado que nunca se revela, y de que se publique una "clave pública" correspondiente a otras partes. Por ejemplo: Alicia firma un mensaje con su clave privada; posteriormente, tras recibir el mensaje, Roberto puede verificar la firma de Alicia utilizando la clave pública de ella. Esta asimetría, plasmada en la distinción entre claves privadas y públicas, permite muchas nuevas primitivas que no pueden existir en el paradigma simétrico. Esto incluye no solo las firmas sino también el intercambio de claves Diffie-Hellman, que es esencial para establecer claves secretas compartidas que permitan una comunicación segura cifrada simétricamente.

Las claves pública y privada están estrechamente relacionadas: en esencia, la clave pública presenta una instancia de un problema matemático (como un logaritmo discreto de curva elíptica), y la clave privada representa la solución a ese problema. El problema se elige de tal manera que su resolución es inviable desde el punto de vista informático, o al menos no vale la pena el esfuerzo. Por lo tanto, en general, trabajar con criptosistemas asimétricos significa trabajar con cálculos intensivos en estructuras matemáticas, y esto tiene un alto costo en términos de memoria y energía, un costo que a menudo es simplemente demasiado pesado para las aplicaciones de IoT de gama baja. Mejorar el rendimiento y la aplicabilidad de los criptosistemas asimétricos en el espacio de la IoT constituye una línea de investigación importante.

En el entorno precuántico, la criptografía de clave pública para la IoT está dominada por la criptografía de curva elíptica (ECC). La única ventaja accionable de la ECC son sus llaves especialmente pequeñas: solo bastan 32 bytes para almacenar una clave ECC de alta seguridad, y una firma ECC de alta seguridad cabe en 64 bytes. Sin embargo, el uso de ECC implica la realización de un gran número de cálculos en módulo de enteros de 32 bytes (¡no de 32 bits!). En el ámbito de los PC esto no es un problema, y la ECC es actualmente ubicua en el intercambio de claves y firmas en Internet. Sin embargo, en el ámbito de la IoT de bajo consumo, estos cálculos teóricos de los números suponen una huella de memoria no trivial, un serio drenaje de las reservas de energía y un tiempo de ejecución doloroso con los consiguientes problemas de latencia. Por lo tanto, una de las líneas de investigación más activas es la adaptación de los protocolos ECC y el desarrollo de nuevos algoritmos ECC para hacer más con menos: mantener una alta seguridad para los dispositivos IoT de gama baja y reducir sustancialmente los costos de ejecución.

↗ En Inria, el equipo-proyecto **GRACE** trabaja en la seguridad de canal lateral de los microcontroladores y en primitivas criptográficas eficientes de clave pública (asimétricas), que incluyen primitivas dirigidas a los dispositivos IoT, como el esquema de firma qDSA.

Criptografía asimétrica para la IoT postcuántica

De cara al futuro postcuántico, la criptografía asimétrica se enfrenta a un gran problema: la existencia de computadores cuánticos suficientemente grandes que ejecuten el algoritmo de Shor destruiría la seguridad de prácticamente todas las primitivas asimétricas más utilizadas. La investigación actual tiene como

objetivo desarrollar y estudiar más sistemas de criptografía asimétrica que sean seguros desde el punto de vista cuántico, sobre la base de una amplia variedad de enfoques, incluidos, por ejemplo, los sistemas basados en retículos, en hashes, en código y en isogenia.

El NIST ha iniciado un proceso internacional de varios años de duración para seleccionar los algoritmos propuestos para las firmas postcuánticas y la encapsulación de claves (que básicamente sustituyen al Diffie-Hellman precuántico). Varios de los algoritmos finalistas que se están estudiando ya reducen el tamaño requerido de las claves públicas, las firmas y el costo computacional. Sin embargo, estos algoritmos no fueron diseñados para las aplicaciones de IoT, y su potencia en este ámbito no se ha analizado aún. El desarrollo de esquemas de firma y establecimiento de claves postcuánticas eficientes, prácticos y probados, dirigidos al espacio del IoT, es una fuente de problemas fascinante y muy apasionante para los investigadores en criptografía.

↗ En Inria, los equipos de proyectos **ARIC**, **COSMIQ** y **GRACE** trabajan en el diseño, el análisis y la implementación eficiente de criptosistemas asimétricos post-cuánticos. Los investigadores de Inria también participan en la presentación de propuestas al proceso de normalización postcuántica del NIST.

2.5 Procesamiento de datos y privacidad con la IoT

La IoT permite la recopilación de datos de forma generalizada, el seguimiento de diversos sistemas físicos, la captura de observaciones ambientales, procesos industriales u otras actividades humanas, a menudo en tiempo real.
Por lo tanto, aunque la recopilación y explotación de estos datos impulsa los avances en muchos ámbitos (por ejemplo, la salud y el desarrollo sostenible, por nombrar algunos), la protección de la privacidad se convierte en una cuestión fundamental.

Esta cuestión plantea retos tanto a nivel político como a nivel científico y técnico.

A nivel político y jurídico, las nuevas normativas pueden resolver parcialmente los problemas de privacidad. Entre algunos ejemplos destacados se encuentran marcos como el Reglamento General de Protección de Datos (GDPR) de la UE, las recomendaciones del WP29 y otras directrices similares en materia de ética y confianza.

A nivel científico y técnico, se destacan los desafíos específicos para diseñar técnicas de explotación de datos de IoT que protejan la privacidad de forma intrínseca.

↗ En Inria, el equipo-proyecto **PRIVATICS** trabaja en el seguimiento y la caracterización de la exposición de los datos personales en los casos de uso de la IoT, y diseña mecanismos que mejoran la transparencia para los usuarios de IoT y permiten su consentimiento adecuado.

Paradigmas de protección de la privacidad

La recopilación de datos y la ciencia de los datos son el núcleo de los sistemas de información modernos. Los dispositivos IoT desempeñan un papel fundamental en la recopilación de estos datos.

Sin embargo, la recopilación básica de datos centralizados conduce a un callejón sin salida en cuanto a la privacidad, así como a una carga excesiva de la

red cuando hay que transferir demasiados datos. Por ello, se necesitan nuevos paradigmas y las investigaciones actuales estudian ciertas alternativas.

Por ejemplo, en lugar de compartir sus datos brutos, una entidad puede compartir datos preprocesados. Este enfoque puede funcionar en varios modelos organizativos, por ejemplo cliente-servidor o totalmente descentralizado (peer-to-peer). La motivación de los proveedores de datos recae en tener el control total de la distribución de la información derivada de sus datos. Esto requiere que algunos costos computacionales, de almacenamiento o comunicación se compartan entre más máquinas diversas en diferentes partes de la red, potencialmente en su borde.

Para habilitar el preprocesamiento, primero hay que poder programar los dispositivos IoT. Por lo tanto, existe la necesidad inicial de contar con plataformas adecuadas de software embebido que ofrezcan una base apropiada, tanto en términos de apertura como de rendimiento. Los enfoques para compartir el uso de los datos se pueden basar en técnicas como:

- ***la transformación de los datos*** (por ejemplo, la adición de ruido) para obtener algunas garantías de anonimato (privacidad diferencial, anonimato K, sensibilidad L...),
- ***primitivas criptográficas específicas*** como el cifrado homomórfico para proteger los datos en los cálculos multipartitos, etc.
- ***compresión de datos con pérdidas para ofuscar parcialmente la información*** por ejemplo, comunicar sólo agregaciones de datos, modelos de predicción (parciales) o cálculos intermedios como gradientes o estadísticas, o combinaciones de éstos.
- ***incorporar técnicas de gestión de datos,*** para externalizar los resultados de forma selectiva (por ejemplo, emitir una alerta basada en la ocurrencia de una conjunción de eventos, en lugar de todos los eventos recogidos) y para representar la información recogida (por ejemplo, emitir una estadística calculada, en lugar de extensos conjuntos de datos en bruto).
- ***técnicas de computación confiables*** embebidas (y distribuidas) en dispositivos de hardware de IoT seguros, para certificar que se utilizó el código de procesamiento esperado, junto con los datos de entrada apropiados, para producir un resultado determinado.

El desafío habitual de la privacidad consiste en diseñar mecanismos que maximicen la utilidad de los datos al tiempo que protejan la privacidad. Un reto adicional es minimizar la relación entre el costo y los beneficios de la privacidad para los proveedores de datos, que pueden ser dispositivos IoT con recursos muy limitados.

↗ En Inria, el equipo-proyecto **PRIVATICS** trabaja en el diseño y la implementación de algoritmos para el intercambio de información que protejan la privacidad, aplicable a dispositivos IoT vestibles que van desde los smartphones hasta los tokens inteligentes.

↗ En Inria, el equipo-proyecto **ARIC** trabaja en el diseño y el análisis de esquemas de encriptación homomórfica completa, y en su uso para cálculos que preservan la privacidad.

↗ En Inria, el equipo-proyecto **COMETE** trabaja en el diseño y análisis de esquemas de privacidad diferencial utilizados para los cálculos que protegen la privacidad.

Smart Container, una solución para el seguimiento y la supervisión de los contenedores.
© Photo Raphaël de Bengy.

Aprendizaje automático descentralizado a través de la IoT

SCompartir el uso de los datos en lugar de los propios datos es un principio que también puede mitigar los problemas de privacidad para el aprendizaje automático (ML) que explota datos IoT que son potencialmente delicados en cuanto a privacidad. En este contexto, el aprendizaje federado (FL) es un campo de investigación activo[1], en el que varios clientes colaboran a través de un servidor central para entrenar un modelo, mientras cada uno mantiene sus propios datos de entrenamiento. El principio es, de nuevo, minimizar la recogida de datos, con el objetivo de eliminar tanto los problemas de privacidad como los cuellos de botella en la red (cuando hay que transferir demasiados datos[2]). Un desafío crucial que se plantea aquí es la falta de una autoridad central que controle y distribuya los datos entre usuarios. Dado que los datos permanecen en el lugar en el que se recogieron, los algoritmos de ML que integran los sistemas de decisión tienen que tratar con datos no idénticos y distribuidos (dii). De hecho, la suposición de lo "idéntico" es lo principal para que el ML afirme que el modelo aprendido se comportará según lo esperado para los valores futuros y que la propiedad "independiente" simplifica mucho la complejidad de la clase de modelos posibles.

Otros estudios analizan el aprendizaje federado totalmente descentralizado, sin un servidor central, de forma parecida a los sistemas peer-to-peer. Dentro de este contexto surge la oportunidad de aprovechar el número masivo de usuarios para mejorar la privacidad. Sin embargo, uno de los principales desafíos es saber con quién colaborar y cómo optimizar los costos de comunicación. Aquí surgen los típicos problemas de seguridad y confianza P2P, que se deben revisar y mitigar en este contexto (por ejemplo, la detección de usuarios maliciosos, la colusión entre usuarios). También surgen problemas específicos en función de las técnicas de protección de la privacidad: por ejemplo, si se añade ruido para ofuscar parcialmente los datos que se comparten, su eficacia podría reducirse drásticamente cuando se dispone de pocos datos. Finalmente, pero no por ello menos importante, el cómputo y el estado (modelo y datos de entrenamiento) se deben minimizar para que se ajusten a los recursos más reducidos con los que cuentan los usuarios de IoT de gama baja.

1. Peter Kairouz et al. Advances and Open Problems in Federated Learning. Technical report, arXiv:1912.04977, https://arxiv.org/abs/1912.04977, 2019.
2. Por ejemplo, los vehículos autónomos equipados con cámaras y sensores recogen una enorme cantidad de datos, y en varios puntos la conexión a la red es intermitente.

↗ En Inria, el equipo-proyecto **MAGNET** trabaja en el diseño de métodos para el aprendizaje automático (ML) respetuoso con la privacidad. Lo anterior se hace mediante técnicas de anonimización de datos para alimentar el ML, y la utilización de algoritmos peer-to-peer totalmente descentralizados, que relajan los supuestos centrales del aprendizaje colaborativo o federado.

Computación de base de datos confiables descentralizadas en la IoT

El procesamiento de bases de datos, y en particular de Big Data, es de suma importancia en el contexto de la IoT. Compartir el "uso" de los datos en lugar de los datos mismos conduce a un nuevo paradigma, en el que las operaciones de procesamiento de datos se trasladan al borde de la red y, en el extremo, dentro de los propios dispositivos de la IoT. Este enfoque favorece la confidencialidad y la privacidad de los datos (especialmente mediante la aplicación local de reglas de control de acceso y confidencialidad), así como el ahorro de energía, al evitar la transmisión de datos de uso poco frecuente, y la generación de resultados agregados en lugar de la totalidad de los datos brutos recopilados.

Desde el punto de vista de las bases de datos, esto nos lleva a considerar grandes conjuntos de objetos IoT (dotados de recursos de almacenamiento y computación) como una base de datos distribuida o federada, sobre la que se puede ejecutar el procesamiento global de la base de datos. Los desafíos de investigación que plantea esta visión son los siguientes:

- (1) hacer que las técnicas de bases de datos (almacenamiento e indexación, algoritmos de evaluación de consultas) sean compatibles con las serias restricciones de hardware que conllevan los objetos inteligentes y, especialmente, con la poca RAM con la que se dispone en comparación con las grandes cantidades de memoria Flash;
- (2) diseñar nuevas técnicas de evaluación de consultas distribuidas seguras en dispositivos IoT, a muy gran escala sin recurrir a un servidor central de confianza.

El primer desafío se deriva de las restricciones de hardware contradictorias de los dispositivos IoT con respecto a las técnicas de gestión de datos: la escasa memoria RAM exige que se indexen los datos de forma masiva (porque los resultados intermedios no se pueden generar en la memoria RAM durante la ejecución), pero la especificidad de la memoria NAND Flash penaliza las pequeñas escrituras aleatorias (que son necesarias para mantener los índices). En Inria se están llevando

a cabo trabajos innovadores con el fin de resolver estas limitaciones, para poder almacenar y procesar millones de entradas de bases de datos almacenadas en un objeto inteligente gracias a nuevos principios de diseño. El siguiente desafío en materia de investigación es generalizar estos resultados al caso de las series de datos, el principal tipo de datos presente en los dispositivos IoT.

En cuanto al segundo desafío, se puede establecer un paralelo con las federaciones de datos privados. Se trata de un área de investigación activa en materia de bases de datos, en la que el objetivo para un conjunto de propietarios de datos es contribuir con sus propios datos para responder a una consulta global, sin revelar los datos (potencialmente sensibles) de cada uno. Actualmente se investigan varios enfoques, en los que se recurre a diversas técnicas como la criptografía (cálculo seguro multipartito), la adición de ruido (privacidad diferencial) o la computación de confianza (seguridad basada en el hardware). La transposición de estas técnicas en el marco de la IoT es difícil, ya que implica disponer de enormes conjuntos de "propietarios de datos" (potencialmente millones de objetos inteligentes implicados) que estén sujetos a limitaciones en cuanto a recursos y gasto energético. Algunos estudios preliminares se basan en el hardware seguro que tienen algunos dispositivos IoT (por ejemplo, chips seguros o TPM) para manejar algunos cálculos de Big Data (MapReduce) con garantías de confidencialidad e integridad, aunque el tema sigue constituyendo una amplia vertiente de investigación.

En términos más generales, las soluciones a estos desafíos permiten devolver a los individuos la capacidad de decisión sobre sus datos personales y ayudar a los ciudadanos a contribuir colectivamente a la computación de bases de datos de cualquier tipo (SQL, Big Data, IA, etc.) de forma fiable, sin tener que recurrir a ningún tercero de confianza de forma obligatoria.

↗ En Inria, el equipo-proyecto **PETRUS** trabaja en el diseño de una arquitectura de bases de datos de confianza para los Sistemas de Gestión de Datos Personales (PDMS, por sus siglas en inglés), con garantías de seguridad y privacidad, que permita realizar consultas distribuidas con conjuntos muy grandes de PDMS. **PETRUS** ha desarrollado PlugDB, una plataforma de hardware y software de PDMS que utiliza tecnologías de hardware y microcontroladores de confianza.

2.6 Seguridad, fiabilidad y certificaciones para la IoT

Una IoT en su desarrollo máximo aumentará nuestra dependencia vital sobre sistemas embebidos, sobre sensores y actuadores conectados en red. En muchas aplicaciones, el término "vital" se utiliza de forma literal, porque con la IoT los dispositivos digitales pueden provocar efectos físicos directos.

Está surgiendo una tendencia de implantes inteligentes que incluye hardware embebido de consumo, un bucle de red inalámbrica y código abierto. Por ejemplo, los sistemas de páncreas artificiales (APS) están diseñados para que ajusten automáticamente el bombeo de una bomba de insulina basal, con el fin de mantener la glucosa en sangre en un rango seguro durante la noche y entre las comidas. Si el APS se avería, la vida del paciente corre peligro inmediatamente.

En términos más generales, una serie de incidentes de seguridad y fiabilidad de la IoT que se han producido recientemente afectan a una gran variedad de máquinas, incluidos vehículos como automóviles conectados e incluso aviones. Debido a las fallas de la IoT, las vidas de los usuarios corrieron peligro o fueron víctimas de accidentes fatales. En conjunto, la cadena de incidentes más recientes apunta a lo siguiente:

- incluso el código más seguro puede contener errores fatales o explotables;
- incluso el código fuente cerrado y altamente sensible se puede filtrar.

A medida que los casos de uso de la IoT se extienden más allá de artefactos divertidos, los aspectos de seguridad de la IoT adquieren mayor relevancia. Los problemas surgen porque es probable que los dispositivos IoT se utilicen de formas imprevistas, o en contextos potencialmente hostiles, propensos a los ciberataques. Combinar los requisitos de seguridad de la IoT con sus requisitos de protección supone un reto abrumador. Un ejemplo ilustrativo es la certificación: a menudo, un producto IoT es un objetivo móvil (debido a las actualizaciones de software) y el contexto en el que se utiliza no está restringido (por ejemplo, la electrónica de consumo). Entonces, ¿qué hay que certificar exactamente y cómo?

Para hacer frente a los desafíos en este ámbito, las comunidades de investigación sobre seguridad y protección –que tradicionalmente son bastante distintas– deben colaborar más estrechamente y revisar juntos los conceptos

fundamentales, desde la base.

Por un lado, garantizar la seguridad y la protección ya no es una tarea "en solitario". Implica a un complejo conjunto de partes interesadas: proveedores de software, operadores, reguladores, usuarios individuales, etc. En tales contextos, los marcos legales deben poder determinar quién es responsable de qué. Por otro lado, la mayor interdependencia entre sistemas obliga a replantearse lo que se considera "crítico". Por ejemplo, los estudios han demostrado que una red de bots medianos de acondicionadores de aire y calefactores habilitados para la IoT pueden ser un arma para interrumpir una red eléctrica nacional. Por lo tanto, uno de los retos es la seguridad de un sistema mixto que incluya no sólo componentes críticos tradicionales, sino también componentes IoT económicos y de bajo consumo. La certificación necesaria para este tipo de componentes supone un reto no sólo porque es difícil de formalizar en este contexto (¿qué es una ciberseguridad suficientemente buena?), sino también porque tiene que seguir siendo muy rentable, ya que se trata de dispositivos baratos.

Mapa de la sala de IoT en el Laboratorio de Lyon. © Photo C. Morel.

2.7 Interacción humano-máquina con la IoT

Con la IoT, los computadores "desaparecen" cada vez más y la interacción máquina a máquina (M2M), cada vez más compleja, ocurre "bajo el capó". Mediante sensores y actuadores, y a medida que la interacción con el sistema adopta nuevas formas (por ejemplo, basadas en el gesto), la propia realidad física se puede personalizar y experimentar de forma diferente. La postfenomemología estudia la interacción entre los seres humanos, el mundo y las tecnologías modernas, estas últimas como mediadores no neutrales. Paradójicamente, en el caso del M2M, el factor humano se vuelve aún más crucial. A medida que se prescinde más sistemáticamente de los humanos para conseguir más beneficios, éstos se pueden ver más afectados por un mal funcionamiento del sistema, o por la falta de comprensión sobre su funcionamiento. Por ejemplo, los trabajadores corren cada vez más el riesgo de ser descalificados o incluso sustituidos.

A medida que la IoT se generaliza, se corre el riesgo de que ésta genere una nueva brecha digital, en la que algunos usuarios se ven gravemente perjudicados por la tecnología, otros adquieren un control más detallado y otros ganan poder a través del control inteligente de las API. Así, el diseño adecuado de la nueva interacción humano-máquina es fundamental

Dotar a los humanos de los niveles adecuados de control sobre la IoT (¿cuál es el nivel correcto?)

Veamos un ejemplo: los termostatos. Los termostatos se diseñaron inicialmente para controlar la temperatura, normalmente con interfaces minimalistas como un mando giratorio, sin que hicieran nada más. En la IoT, estos dispositivos pueden tener muchas más capacidades y funcionalidades: se pueden programar, utilizar para controlar algunos otros sistemas, enlazar con otros dispositivos o sensores, o con algún servicio online, etc. Sin embargo, aunque estén potenciados por la IoT, muchos de estos dispositivos conservan la interfaz minimalista original. Este enfoque de adaptación a lo anticuado plantea una serie de problemas. Por un lado, estas interfaces son fáciles de usar y resultan familiares. Por otro lado, las

interfaces sustitutivas básicas (por ejemplo, a través de la pantalla de un smartphone) no alcanzan el pleno potencial de las interacciones ciberfísicas. Aunque los aspectos tecnológicos de embeber la tecnología en el mundo real están muy avanzados, aún no hemos conseguido una transición fluida entre ambos.

Entendiendo lo que ocurre "bajo el capó" de la IoT

Lograr un nivel adecuado de transparencia se relaciona con la forma en que los usuarios entienden la IoT. Las infraestructuras de la IoT son intrínsecamente complejas, formadas por nodos heterogéneos interconectados y dispositivos interactivos, con una "inteligencia ambiental" subyacente. Esta complejidad plantea retos en términos de interacción, para que los usuarios puedan controlar dichos sistemas. La tendencia general de las últimas décadas en las tecnologías interactivas ha sido simplificar en exceso las interfaces para hacer más sencilla la interacción. Sin duda, esto ha contribuido a democratizar el uso de la tecnología para los novatos digitales, pero a costa de una menor expresividad. En el contexto de la IoT, es probable que este enfoque no se extienda debido a la complejidad de las infraestructuras y los medios particulares de interacción que ofrecen (por ejemplo, múltiples dispositivos, entrada/salida reducida, interacción distante y distribuida).

Uno de los retos es, por ende, acomodar mejor la complejidad mediante el diseño de interfaces e interacciones adecuadas para que los usuarios puedan construir progresivamente un modelo mental apropiado del sistema, es decir:

- comprender y anticipar cómo reaccionará el sistema a sus acciones;
- tener una visión clara y correcta de los estados y errores actuales del sistema; y
- adquirir habilidades de forma paulatina para poder controlar el sistema con precisión.

Otro desafío es el del control compartido. Los sistemas IoT suelen tener cierto grado de autonomía y pueden tomar la iniciativa para realizar tareas o proponer acciones a los usuarios. Este punto puede resultar crítico. Los usuarios deben conocer el estado actual del sistema, ya que puede haber cambiado de forma autónoma; los usuarios deben saber cómo pueden recuperar el control cuando sea necesario; y cuando el sistema actúe por sí mismo, los usuarios deben sentir que tienen el control. En concreto, los usuarios deben poder:

- identificar las acciones adecuadas y comunicar sus intenciones;

- confiar en el sistema en cuanto a su coherencia ante situaciones similares; y
- controlar el sistema de manera que se puedan identificar y corregir los errores.

Algunos ejemplos de control compartido que salieron espantosamente mal son los accidentes del Boeing 737MAX, debidos en parte a que se ocultó un comportamiento no documentado "bajo el capó". La investigación en el campo de la interacción humano-computador (HCI, por sus siglas en inglés) ha comenzado a analizar incidentes de este tipo, con el objetivo de caracterizar la comprensión y la visibilidad de los usuarios acerca de los estados del sistema.

Una de las dificultades es que el sistema controla al usuario, más que el usuario al sistema. Sin embargo, se podría aprovechar un enfoque basado en la inteligencia computacional mediante el seguimiento y la inferencia de tareas para anticipar las acciones del usuario, lo que eliminaría la necesidad de una interfaz explícita y siempre habilitada. Una de las promesas de la tecnología ubicua, que se exploró por primera vez con la investigación sobre el Escritorio Digital de Welner, han sido los entornos que se anticipan al usuario. Básicamente, a través de modelos de usuario y tarea, el entorno se reconfigura automáticamente mientras el usuario permanece en control. En última instancia, estos enfoques también podrían apoyar la adaptación de las interfaces a varios tipos de público, al ofrecer a los usuarios niveles adecuados de controles según sus necesidades, habilidades y contextos de uso.

↗ En Inria, los equipos de proyectos tales como **AVIZ**, **EXSITU**, **ILDA** y **LOKI** estudian y diseñan nuevos métodos de interacción y sistemas interactivos que capacitan a los usuarios de mejor manera, en base a sus capacidades y conocimientos.

Aprovechar el potencial de la interacción aumentada físicamente

La investigación sobre la interacción táctil y tangible muestra un potencial considerable para ampliar las (hasta ahora) escasas capacidades de entrada que suelen caracterizar a los dispositivos IoT. Es más, la investigación en HCI (Interacción Humano-Computador) no para de buscar técnicas de detección avanzadas que puedan detectar y diferenciar las formas en que tocamos una superficie (por ejemplo, identificación de los dedos, detección precisa del punto de contacto, presión aplicada, inclinación de los dedos). Del mismo modo, la forma en que se toma y manipula un objeto físico puede informar mucho sobre la intención del

usuario. Por ejemplo, imaginemos un estuche de lápices: uno lo coge de forma diferente si la intención es abrirlo, guardarlo o entregárselo a otra persona. Este principio se aplica a otros objetos, y los dispositivos IoT no son la excepción. Junto con los estudios sobre la capacidad de los usuarios para aprovechar las tecnologías de detección táctil y tangible, la investigación sobre enfoques físicamente aumentados pretende mejorar el ancho de banda de la interacción entre los usuarios y los dispositivos IoT sin ninguna interfaz adicional/externa: un solo botón podría, por ejemplo, desencadenar diferentes acciones según la forma en que se toque o se pulse.

Sin embargo, estos enfoques sólo abordan parcialmente los problemas que surgen de la visibilidad limitada que se tiene de las diferentes acciones que se pueden realizar en el sistema, y la falta de proalimentación (feedforward o qué hacer) o retroalimentación (qué se hizo) del mismo. Por un lado, hacer la interacción "física" podría ayudar al usuario a transferir conocimientos de otros contextos. Por otro lado, aumentar las capacidades de interacción (por ejemplo, añadiendo la detección táctil a un botón físico) podría contribuir a mejorar la visibilidad y la capacidad de descubrimiento de las acciones y funcionalidades. Aquí es donde la Realidad Mixta (MR, por sus siglas en inglés) ofrece una manera prometedora de hacer reaparecer estas "interfaces invisibles", por ejemplo, con teléfonos inteligentes o dispositivos vestibles como gafas, que superponen pistas sutiles sobre la interacción con los dispositivos físicos, o incluso mediante la superposición de tutoriales completos, a petición del usuario.

La MR también podría ayudar a proporcionar a los usuarios una mejor retroalimentación del sistema, que también se podría complementar con soluciones hápticas como la retroalimentación vibrotáctil. Una línea de investigación muy activa en HCI relacionada con la interacción con dispositivos IoT se centra en la búsqueda de nuevas formas de habilitar dicha retroalimentación en cualquier superficie (por ejemplo, actuadores, electrovibración), y en la comprensión de cómo los usuarios los perciben y qué tipo y cantidad de información pueden transmitir. Otra área es la detección del movimiento humano como apoyo a una amplia gama de aplicaciones de rehabilitación y creatividad.

↗ En Inria, los equipos de proyectos tales como **AVIZ**, **EXSITU**, **ILDA** y LOKI estudian nuevos materiales y dispositivos interactivos con el fin de crear nuevas formas de interfaces tangibles para una amplia variedad de aplicaciones domésticas, laborales y creativas.

2.8 Control con la IoT

Uno de los principales objetivos de la IoT es permitir la supervisión y el control avanzados de los sistemas distribuidos que se despliegan en diversos entornos (desde el hogar y los edificios inteligentes hasta las ciudades inteligentes y la industria 4.0). En particular, la IoT tiene el potencial de aportar una supervisión y un rendimiento avanzados mediante un control optimizado a los sistemas de pequeña escala que no pueden costear los sistemas de control dedicados.

El uso de redes compartidas multipropósito para controlar elementos espacialmente distribuidos resulta en arquitecturas muy flexibles. El inconveniente es que se añaden dinámicas asíncronas en los bucles, lo que puede degradar mucho el rendimiento e, incluso, la estabilidad. La estimación de los efectos de la red y el diseño de sistemas robustos de control en red (NCS, por sus siglas en inglés) es un reto motivador, que implica sistemas híbridos que mezclan estados continuos y eventos discretos, sistemas de retardo, etc. Los algoritmos también deben gestionar jerarquías complejas de subsistemas que involucran esas dinámicas asíncronas y multiescalares con escalas de tiempo extremadamente variadas (desde meses hasta microsegundos) y un alcance geográfico extremadamente variado (desde dentro de un chip hasta el planeta entero). El diseño del control de bucle cerrado en estas redes no deterministas impone una ultrarresistencia frente a las variaciones (inevitables) en términos de latencia, fluctuación (jitter) y rendimiento.

↗ En Inria, el equipo **VALSE** trabaja en el modelado y análisis de sistemas dinámicos inciertos y altamente distribuidos que se encuentran en los sistemas IoT y ciberfísicos. **VALSE** diseña algoritmos de estimación robusta y control descentralizado mediante los conceptos de convergencia y estabilidad en tiempo finito/tiempo fijo/hiperexponencial.

Un **reto relacionado en este campo es la gestión autónoma del bucle de retroalimentación en el middleware de la IoT.** Normalmente, el control y la monitorización de la IoT implican el uso de middleware para la supervisión y gestión de la infraestructura. El middleware de la IoT tiene como objetivo permitir la gestión centralizada o distribuida de componentes lógicos complejos y distribuidos, en infraestructuras muy heterogéneas (por ejemplo, pequeños dispositivos con potencia de cálculo limitada, pasarelas domésticas, nodos locales de una red celular o centros de datos en la nube). Por lo tanto, el middleware de la IoT debe proporcionar abstracciones utilizables para la gran variabilidad de los sistemas operativos y los protocolos de comunicación.

Una cuestión fundamental en este ámbito es la automatización de los bucles de retroalimentación ciberfísicos, por ejemplo, con la computación autónoma. Estos bucles de control tienen por objeto permitir la autoadaptación continua del sistema ciberfísico, reaccionando a la información supervisada con decisiones, que se toman sobre la base de una representación del sistema, y se aplican mediante acciones, con el fin de aplicar una estrategia o política de alto nivel. Esto se realiza frente a las (potencialmente elevadas) dinámicas que ocurren tanto en el entorno físico que se monitorea y controla (que es el objeto clásico de la Teoría del Control), como en la propia infraestructura del sistema de computación y comunicación (por ejemplo, la variación de la carga, la tolerancia a los fallos, la autoprotección).

↗ En Inria, el equipo-proyecto **ACENTAURI** trabaja en nuevos paradigmas que aumentan la autonomía de los sistemas robóticos, permitendo un comportamiento orientado a las tareas y aprovechamiento de la percepción y el control multisensoriales.

Los retos incluyen el diseño y la optimización de esquemas de reconfiguración automática y arquitecturas de software para los aspectos funcionales a nivel de aplicación, así como para los aspectos computacionales a nivel de infraestructura (por ejemplo, migración de servicios, autoescalamiento), con requisitos de separación de preocupaciones entre estos diferentes niveles.

↗ En Inria, el equipo-proyecto **CTRL-A** trabaja en el diseño de métodos para controladores de computación autónoma, sacando provecho de la Teoría de Control para permitir la gestión de las arquitecturas reconfigurables de computación, tanto en la IoT como en la HPC.

Reducción de la brecha entre la robótica y la IoT industrial

Los microrrobots están surgiendo como herramientas de bajo consumo, baratas y diminutas, cuyo tamaño permite nuevas aplicaciones en robótica. Los enjambres coordinados de estos diminutos robots despiertan especial interés. Los enjambres tienen el potencial de superar a los robots monolíticos en aplicaciones en las que la diversidad espacial conlleva ventajas, como la detección distribuida. La robótica de enjambre se puede considerar como la próxima frontera de la investigación de la IoT industrial, ya que requiere abordar muchas de las cuestiones de investigación abiertas, simultáneamente, para permitir el control y la interacción con un gran número de microrrobots.

Un primer reto es la movilidad. Aunque los protocolos de IoT de bajo consumo se han estandarizado bastante y se están desplegando, se diseñaron principalmente para interconectar dispositivos desplegados de forma estática en una misma zona. Hacer que algunos de estos dispositivos, o todos ellos, se desplacen no es algo que se admita adecuadamente en los protocolos estándar de la IoT industrial actual (como el 6TiSCH).

Plataforma experimental FIT (Future Internet of Things). © Inria / Photo C. Morel.

Un segundo reto es la latencia baja y predecible. En la actualidad, las redes industriales de IoT pueden garantizar que los datos generados se entreguen, por ejemplo, a una pasarela. Pero aunque la latencia nunca se puede garantizar (la tecnología inalámbrica no es fiable), la programación que se plantea en la red permite que la latencia sea predecible. Este determinismo ofrece la posibilidad de ejecutar bucles de control a través de las redes de IoT, como se ha destacado anteriormente.

Un tercer reto es la localización precisa y frugal. Se han desarrollado técnicas de localización fundamentales, como el ángulo de llegada UWB o BLE. Un reto de investigación vigente es codiseñar la solución de localización con los protocolos de comunicación, lo que da lugar a una localización bajo demanda que es compatible con los requisitos de bajo consumo de la mayoría de las aplicaciones de IoT.

↗ En Inria, el equipo-proyecto **EVA** trabaja en la robótica experimental de enjambre. Por ejemplo, **EVA** ha desarrollado el simulador de enjambre robótico Atlas y está construyendo DotBot, un gran banco de pruebas para enjambres de robots a escala centimétrica de hasta 1.000 unidades. El equipo-proyecto **AVIZ** trabaja en el diseño de enjambres de robots diminutos capaces de realizar visualizaciones físicas y otras tareas diversas. Por ejemplo, AVIZ ha diseñado Zooids.

2.9 La seguridad en la IoT

Los ciberataques que involucran a entidades que cruzan las fronteras nacionales son ahora la nueva normalidad. La piratería en línea, con fines de lucro e impulsada por gobiernos, está alcanzando niveles sin precedentes: la Tercera Guerra Mundial se lucha en línea. También existe una tendencia actual a que la mayoría de los delitos incluyan algunos componentes ciberfísicos.

En este contexto, los retos de seguridad surgen y son transversales a todos los aspectos de la IoT. Dado que la seguridad y la resistencia son tan fuertes como los eslabones más débiles, asegurar la IoT de baja potencia se vuelve aún más crucial.

Más allá de los ataques de ciberseguridad más básicos (phyishing, ingeniería social, etc.) una creciente variedad de ataques, requieren mitigación y nuevos mecanismos de seguridad en todos los niveles del sistema.

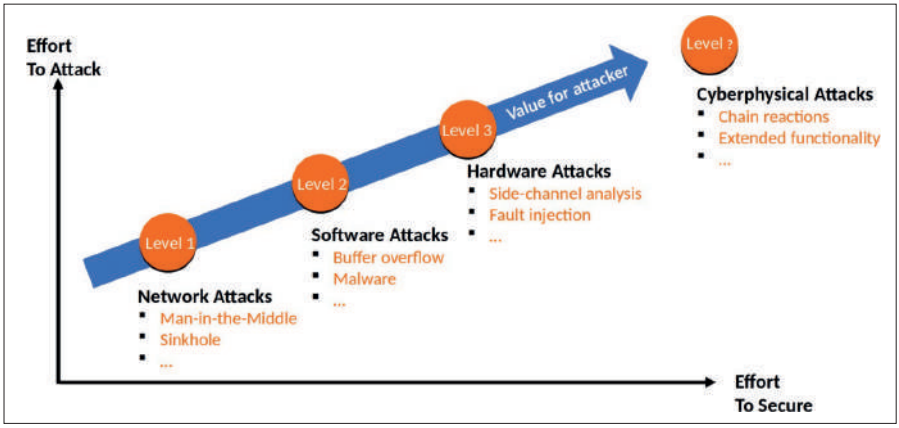


Figure 1: Superficie de ataque en la IoT.

Modelado de los atacantes en la IoT

Los modos de operación de los ciberataques tradicionales siguen siendo efectivos con la IoT: secuencia de intentos para explotar diferentes vulnerabilidades, escalamiento progresivo de privilegios, etc. Sin embargo, la evaluación del riesgo cambia significativamente con la IoT. Si nos rodean cada vez más actuadores controlados por la IoT, que influyen físicamente en nuestro entorno (o incluso en nuestro estado biológico, por ejemplo, un implante inteligente), los niveles de riesgo que toleramos son significativamente menores. Si los sensores mejorados

por la IoT recopilan datos cada vez más íntimos y detallados (piense en su ritmo cardíaco y de transpiración, en tiempo real), el impacto de las violaciones de la privacidad se torna considerablemente mayor.

En cuanto a la seguridad informática tradicional, es necesario abordar una enorme superficie y ámbito de ataque, que abarca desde los ataques de red (man-in-the-middle, sinkhole, etc.), hasta los ataques de software (malware, desbordamiento de búfer) y de hardware (inyección de fallos, canal lateral, etc.), por no mencionar el vector humano y los ataques de ingeniería social. Pero con la IoT aparecen nuevos vectores de ataque.

Ahora es posible provocar reacciones en cadena ciberfísicas catastróficas a distancia, efectos dominó que explotan masivamente las redes de bots y la creciente interdependencia entre sistemas que antes estaban aislados unos de otros, como la red eléctrica e Internet. Por otro lado, los ataques de funcionalidad extendida pueden convertir un dispositivo controlado por la IoT en un arma, transformando su uso de una manera completamente inesperada. Estos ataques amplían aún más la superficie de ataque tradicional de los sistemas en red.

Además, a medida que surgen nuevas interfaces ciberfísicas de usuario, también ofrecen nuevos vectores de ataque. Por ejemplo, la irrupción de los comandos de voz permite nuevos ataques a los asistentes personales de voz, ya que la autentificación de la asistencia de voz por parte del usuario (o viceversa) es difícil y podría ser fácilmente abusada. En un futuro cercano, se espera que las nuevas interfaces ciberfísicas de usuario incluyan implantes inteligentes avanzados similares al prototipo de interfaz ciberfísica cerebral Neuralink, lo que elevará la apuesta en términos de requisitos de seguridad y protección.

Por lo tanto, un reto crucial es definir nuevos modelos de atacantes que capten este contexto.

Aseguramiento de los protocolos de red en la IoT

Los beneficios que aporta la IoT se basan en la incorporación de nuevos dispositivos a través de la red, que antes no existían o funcionaban de forma autónoma y aislada. Por otra parte, estos beneficios tienen el precio de abrir nuevas vías para los ciberataques a través de la red. Por lo tanto, es esencial dar seguridad a las comunicaciones de la red en la IoT.

La pila o stack de comunicación de la red se divide tradicionalmente en capas abstractas. Cada capa proporciona servicios a la capa superior y utiliza los servicios de la capa directamente inferior. El modelo dominante es el de la Internet actual, que consta de las capas de aplicación, transporte, red, enlace y física. Se necesitan mecanismos de seguridad específicos en cada capa de la pila de protocolos de red.

Para comprender los retos en este contexto, primero hay que comprender algunas peculiaridades de los dispositivos y redes de la IoT, comparadas con las máquinas promedio conectadas en el borde de Internet.

TASAS DE TRANSFERENCIA DE DATOS DIMINUTAS

Las redes locales de IoT (o del final de la IoT) a menudo se basan en radios de baja potencia, que presentan limitaciones inusuales en cuanto a la velocidad de datos físicos: desde los 250 kilobit/s anunciados para las tecnologías de corto alcance (que proporcionan conectividad en un radio de 10 metros en interiores, 100 metros en exteriores), hasta aproximadamente 10 kilobit/s para las tecnologías de largo alcance (que proporcionan un rango de conectividad de hasta 10 km en exteriores). A grandes rasgos, esto supone entre el 0,01% y el 0,1% de las tasas de datos anunciadas para el WiFi moderno, o redes celulares 4G.

PATRONES ESPECÍFICOS DE TRÁFICO DE DATOS

Los datos originados en los dispositivos IoT suelen almacenarse en intermediarios antes de llegar a su consumidor final. Por lo tanto, ya no basta con confiar en los datos basándose en la identidad de los otros pares que se comunican, como se suele hacer en la Internet tradicional. En vez, se necesita un modelo productor-consumidor a efectos de seguridad, que ofrezca garantías de seguridad en la capa de aplicación.

PRESUPUESTOS MICROSCÓPICOS PARA LOS RECURSOS DE A BORDO

Los dispositivos de las redes IoT tienen un presupuesto muy reducido en términos de potencia, procesamiento o memoria. Por ejemplo, en términos de memoria, es el 0,001% del presupuesto de recursos disponible en una máquina tradicional conectada a Internet.

UN FACTOR HUMANO DIFERENTE

Los dispositivos IoT de bajo consumo suelen carecer de interfaces de usuario comunes, como una pantalla o un teclado. Al ser los pulsadores y los LED el único medio para interactuar con un dispositivo, la configuración en terreno (para la puesta en marcha o la depuración) se vuelve significativamente más difícil. Además, los dispositivos IoT tienden a tener una relación intrínseca de 1:N con los humanos (piense: todos sus sensores/actuadores/implantes y dispositivos inteligentes),

mientras que otras máquinas conectadas en el borde de la red tienden más a 1:1 (piense: su smartphone, su portátil).

Puesta en marcha de la seguridad, sin interfaz de usuario

Un supuesto común para las soluciones de seguridad de las comunicaciones definidas por los organismos de normalización es que la relación de confianza entre las diferentes entidades involucradas en la comunicación ya se ha establecido a través de claves comunes. En el momento de la fabricación, la relación de confianza se suele establecer entre el dispositivo IoT y el fabricante. Sin embargo, el dominio donde se instalará el dispositivo IoT no se conoce en el momento de la fabricación. Antes de que el dispositivo IoT se pueda unir a un dominio determinado, es necesario aprovisionarlo con credenciales específicas del dominio. La creación de esta relación de confianza entre el dispositivo IoT y el propietario del dominio se suele considerar fuera del alcance de los organismos de normalización; sin embargo, no se trata de una tarea trivial, ya que la mayoría de los dispositivos IoT carecen de interfaces de usuario habituales (pantalla, teclado, entre otros). Pedir una contraseña a un dispositivo IoT de gama baja simplemente no es una opción y se favorece el uso de mecanismos de autenticación automáticos. Las empresas suelen recurrir a canales fuera de banda (por ejemplo, comunicación de campo cercano, red inalámbrica ad hoc, claves precompartidas impresas en la parte posterior de un dispositivo, puerto serial). En primer lugar, este enfoque abre varias vulnerabilidades, ya que el protocolo de "arranque" se acaba diseñando internamente, sin una revisión exhaustiva por parte de la comunidad y los expertos en seguridad. En segundo lugar, este enfoque no es escalable (piense en el arranque de una comunicación segura para docenas de sensores a la vez...). Uno de los retos es, pues, la definición de protocolos de arranque adecuados que tengan en cuenta, por un lado, las limitaciones de los dispositivos y de la red y, por otro, las limitaciones operativas y el ciclo de vida de los dispositivos de la IoT.

↗ En Inria, el equipo-proyecto **EVA** trabaja en el diseño de protocolos de seguridad sin contacto y en la evaluación del rendimiento de los candidatos a estándares de seguridad de las comunicaciones en los casos de uso de la IoT.

Garantizar el paradigma orientado a los datos de la IoT

Las comunicaciones en Internet se han diseñado para estar orientadas a los puntos finales: interconectar máquinas que responden simultáneamente y establecer la seguridad de los canales de comunicación relativamente duraderos que transportan flujos de datos entre dichos puntos finales de comunicación.

El enfoque tradicional (tanto en las comunidades de estandarización como de investigación) ha sido reducir la sobrecarga de comunicación mediante una codificación más eficiente, pero sin comprometer el nivel de seguridad. Por ejemplo, los investigadores propusieron versiones ligeras de los protocolos IPsec y (D) TLS, que reducen la sobrecarga de comunicación mediante la compresión de los campos del protocolo y que no son críticos para la seguridad.

Sin embargo, en gran medida, la comunicación de la IoT tiene un patrón de tráfico diferente, orientado a los datos: una comunicación puntual (piense: una medición periódica de un sensor, o una actualización de firmware) que involucra a máquinas que pueden estar en modo de ahorro de energía (en reposo) la mayor parte del tiempo, de manera que, en algún punto de su tránsito por la red, los datos de la IoT se almacenarán y descansarán temporalmente en algún repositorio.

Los requisitos que impone este paradigma orientado a los datos sólo se han abordado recientemente mediante un esfuerzo por definir nuevos mecanismos basados en las primitivas de "seguridad de las cosas", que aplican los mecanismos de protección en la capa de aplicación. Hay que definir y estandarizar nuevos protocolos y mecanismos ligeros. Un ejemplo de esto es la investigación en el campo del diseño de protocolos de redes centradas en la información (ICN) y sus extensiones de seguridad. Otro ejemplo es la actividad que se desarrolla actualmente en torno a la normalización de OSCORE para la seguridad de las cosas, es decir, la protección de la transferencia web mediante CoAP, y el protocolo EDHOC para el intercambio de claves en la capa de aplicación. Estas categorías de soluciones prometen una sobrecarga de comunicación atractivamente baja y un soporte nativo para la seguridad de los datos de la IoT mientras están en reposo en algún punto de su tránsito por la red, lo que supone una importante mejora con respecto a las soluciones tradicionales.

No obstante, proporcionar una base común y justa para la comparación de protocolos suele ser una tarea complicada. Un desafío continuo en la comunidad académica sigue siendo establecer y llevar a cabo comparaciones relevantes entre los nuevos protocolos de la IoT y los protocolos tradicionales.

Seguridad de las especificaciones de los protocolos de la IoT menos maduros

Muchas soluciones de IoT (las especificaciones o sus implementaciones) son recientes. La relativa novedad de estos protocolos significa que, en comparación con los protocolos con mayor trayectoria (como TLS, por ejemplo), se han sometido a menos análisis, no sólo a nivel de pruebas de seguridad contra las vulnerabilidades de las especificaciones del protocolo, sino también en cuanto a

la implementación algorítmica eficiente y las optimizaciones.

Por lo tanto, un desafío importante en la comunidad académica es el análisis formal de estas soluciones novedosas y ligeras definidas por los organismos de normalización, como el IETF, que demuestran formalmente las garantías de seguridad anunciadas junto con el rendimiento deseado en términos de eficiencia energética.

↗ En Inria, el equipo-proyecto **PROSECCO** trabaja en el diseño de métodos de verificación formal aplicables a la especificación de protocolos de la IoT de bajo consumo.

Al final, es función del administrador de la red decidir qué combinación de protocolos utilizar, qué implementaciones ejecutar y cómo configurarlas, para mitigar las amenazas de un determinado despliegue. El conjunto de habilidades y el conocimiento de fondo de los administradores de red varían, especialmente con los protocolos más recientes. La experiencia demuestra que los parámetros por defecto a menudo se dejan sin tocar, lo que lleva a vulnerabilidades ya conocidas en el sistema. Por lo tanto, la seguridad de la IoT utilizable requiere no sólo especificaciones robustas, sino también la posibilidad (y la disponibilidad) de implementaciones con garantías de seguridad adecuadas por defecto en todos los dispositivos. Por tanto, un reto es impulsar la coevolución de las especificaciones de los protocolos de la IoT y sus implementaciones, con el fin de obtener una seguridad utilizable.

Detección y gestión de incidentes de seguridad de la IoT

Un aspecto esencial de la seguridad de un sistema distribuido son las capacidades relacionadas con la gestión de redes y servicios. Las auditorías globales del sistema pueden descubrir posibles vulnerabilidades antes de que se exploten. El monitoreo del sistema distribuido puede detectar los incidentes de seguridad cuando se producen. Cuando el sistema incluye componentes ciberfísicos de la IoT, la complejidad y la heterogeneidad del sistema se disparan, y de ahí surgen retos específicos.

Uno de los retos es la recopilación de información relevante (a través del análisis pasivo o activo) que rastrea eficazmente las características y la actividad de los dispositivos IoT en directo, lo que es especialmente difícil de lograr dentro de la utilización de recursos de baja potencia. En este caso, es necesario diseñar

o instrumentar nuevos protocolos, para proporcionar puntos de vista adecuados en los despliegues de IoT.

Otro reto es automatizar el cruce de la información específica recopilada en un despliegue concreto, con las bases de información de seguridad mantenidas globalmente (CPE, CVE, CAPEC, CWE, flujos de información sospechosos...). En este caso, un enfoque prometedor que se está investigando aprovecha las técnicas de aprendizaje automático para automatizar y optimizar la realización de complejas auditorías de seguridad de la IoT, y mejorar la velocidad y la precisión de la detección de incidentes de seguridad de la IoT. La gestión de los incidentes de seguridad de la IoT también plantea retos. Un ejemplo es el diseño de nuevas estrategias de confinamiento de ataques y mecanismos que imitan el aislamiento de fallos en el ámbito de la seguridad.

↗ En Inria, el equipo-proyecto **RESIST** trabaja en el diseño de plataformas de gestión de redes para la IoT y en técnicas novedosas que facilitan las funciones de auditoría y monitoreo, con el fin de automatizar la evaluación de la seguridad en los entornos de la IoT. Por ejemplo, SCUBA es una plataforma diseñada para acelerar las auditorías de seguridad en las cosas heterogéneas conectadas.

Cómo asegurar el software de IoT

Las aplicaciones dirigidas a los casos de uso de la IoT están proliferando. Hasta hace poco, el software de los dispositivos IoT de gama baja era propietario, de código cerrado y, a veces, lo que es peor: se basaba en la seguridad por ocultación, débil por diseño. Existe una tendencia hacia más implementaciones de código abierto para la IoT de baja potencia, cuyo efecto secundario es que la seguridad por ocultación ya no es una opción. Con esta evolución, podemos esperar que la seguridad mejore necesariamente.

Sin embargo, dado que son recientes, las partes críticas de estas implementaciones no se han verificado formalmente en cuanto a las vulnerabilidades a nivel de software. Un reto que tiene por delante la comunidad de la verificación formal es involucrarse en el estudio de estas implementaciones de la IoT. Escribir software seguro es difícil, y no hay un enfoque de verificación que sirva para todo. El principal reto es producir software IoT verificado para dispositivos IoT de gama baja, sin que haya penalizaciones importantes de rendimiento y sin sacrificar la versatilidad (el software IoT de bajo nivel tiende a dirigirse a una amplia variedad de hardware y casos de uso).

↗ En Inria, los equipos de los proyectos **TEA** y **PROSECCO** trabajan en la automatización de las pruebas de los bloques de construcción de software embebidosincrustados en dispositivos IoT de baja potencia. Se hace especial hincapié en probar componentes de seguridad clave, como las primitivas criptográficas, y en verificar la corrección funcional y la seguridad de la memoria de los gestores cargadores de arranque mínimos. Mediante el desarrollo de nuevos flujos de trabajo diseñados en torno al lenguaje formal Fstar, la producción de módulos de software embebido verificados y eficientes dirigidos a hardware de bajo consumo se convierte en algo práctico. Un ejemplo destacado de este tipo de módulo de software de la IoT es la criptobiblioteca HACL.

A priori, es poco práctico (tanto técnica como económicamente) verificar formalmente todo el software que se envía y despliega. Además, aunque algún programa informático se verifique formalmente antes de su despliegue en terreno, el software de la IoT puede seguir teniendo fallos y vulnerabilidades que se puedan explotar[3]. La razón es que el código se prueba contra un modelo de seguridad (suposiciones sobre el atacante, etc.). La verificación previa no ofrece ninguna garantía si el modelo no se cumple en la práctica, porque un dispositivo IoT se utiliza de forma inesperada, o en un contexto inesperado –y lo más probable es que lo haga.

Por lo tanto, es necesario complementar la verificación formal a priori con medidas para actualizar periódicamente el software en los dispositivos IoT, para corregir los errores y las vulnerabilidades que sean descubiertas a posteriori, después de que el software se haya implantado o desplegado. Si bien comprende una característica de seguridad, la actualización del software es también un vector de ataque. Por ejemplo, una actualización de software podría vincular el software legítimo con malware. Por el contrario, una actualización de software funcional y necesaria se podría bloquear porque ninguna parte autorizada proporciona una firma digital. Un reto fundamental para la IoT es, por tanto, el diseño de una cadena de suministro adecuada y segura para el software de la IoT, que debe permanecer en funcionamiento durante toda la vida útil de los dispositivos de bajo consumo.

3. Donald Knuth 1977: "Beware of bugs in the above code; I have only proved it correct, not tried it." http://www-cs- faculty.stanford.edu/~knuth/faq.html

Los retos asociados combinan la investigación sobre criptografía de bajo consumo, software reproducible, autenticaciónatestación remota y diseño de software de sistemas profundamente embebidosintegrados. Aparte de la investigación académica, también se necesitan y se esperan nuevas normas en este ámbito, como demuestran los trabajos actuales sobre las especificaciones SUIT, por ejemplo.

↗ En Inria el equipo-proyecto **TRIBE** trabaja en el diseño de una cadena de suministro de actualización de firmware de IoT segura, adaptada a dispositivos de IoT baratos y de bajo consumo, pero sin comprometer la seguridad.

↗ RIOT-fp es un proyecto de ciberseguridad iniciado por Inria, que se centra en dispositivos IoT basados en microcontroladores y con recursos limitados. RIOT-fp aporta bloques de construcción prácticos para una solución de IoT de código abierto que mejora tanto la durabilidad del software como el equilibrio entre funcionalidad y riesgo, para los usuarios finales. Estos bloques de construcción combinan primitivas criptográficas de IoT de alta velocidad, alta seguridad y baja memoria, marcos que ofrecen garantías para la ejecución de software en dispositivos de IoT de gama baja y una cadena de suministro segura para las actualizaciones de software de IoT a través de redes de baja potencia.

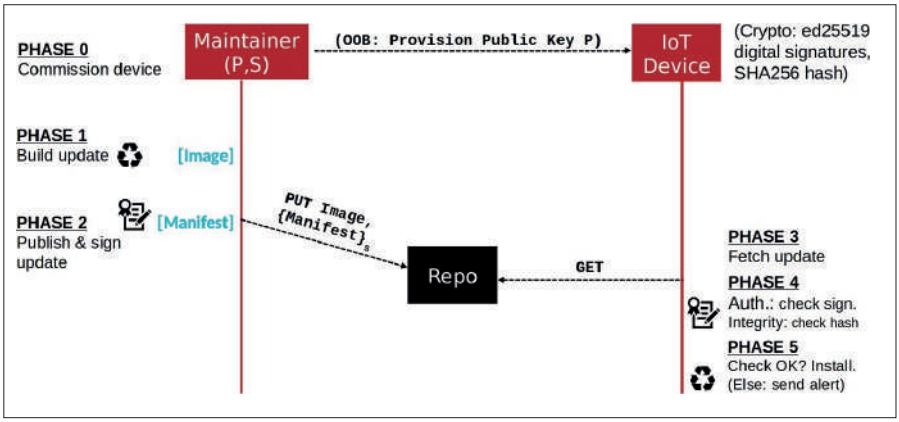


Figura 2: Flujo de trabajo de actualización de software de IoT segura (especificación SUIT en curso).

Cómo asegurar el hardware de la IoT

Por un lado, la flexibilidad intrínseca de las aplicaciones de la IoT que operan en un entorno multiestándar exige la interoperabilidad, la facilidad de uso y las facilidades de actualización de los productos que normalmente sólo ofrece el desarrollo de software de alto nivel. Por otro lado, la aceleración por hardware (HW) puede aumentar la eficiencia energética en varios órdenes de magnitud, mientras que los enfoques puramente de software (SW) suelen ser incompatibles con las limitaciones de recursos incorporados en las placas de los dispositivos IoT.

El diseño híbrido inteligente –arquitectura mixta HW/SW– representa, por lo tanto, una línea prometedora que hay que seguir explorando. Algunos ejemplos de funcionalidades críticas para las que es necesario un diseño híbrido incluyen (pero no se limitan a) la criptografía de la IoT.

Por otro lado, el hardware también ofrece una superficie de ataque que se debe mitigar mediante mecanismos específicos. Especialmente, en el caso de la IoT de bajo consumo, es necesario reevaluar el acceso físico y la seguridad de los dispositivos. Comparado con la captura física de su smartphone o portátil, puede resultar más fácil para los atacantes capturar algún dispositivo IoT (pensemos en una de las docenas de sensores/actuadores repartidos por los alrededores) y someter este hardware a elaborados ataques de canal lateral. En este contexto, los desafíos incluyen:

- nuevos aceleradores de HW para funciones de seguridad (criptografía simétrica y asimétrica, hashing, autenticación, firma, generación de números aleatorios, etc.), con un enfoque específico en la eficiencia energética y el consumo ultrabajo;
- un criptoprocesador especializado que incluya protección contra ataques como la aleatorización;
- optimización de compiladores destinados a criptoprocesadores con recursos limitados;
- traducción binaria dinámica acelerada por hardware (DBT) como medio para mejorar la protección del software; y
- nuevas técnicas para la protección eficiente del hardware contra los ataques de canal lateral y la inyección de fallos, tanto en SW como en HW.

↗ En Inria, el equipo-proyecto **CAIRN** trabaja en la aceleración por hardware de primitivas criptográficas de bajo consumo, así como en arquitecturas de criptoprocesadores energéticamente eficientes con contramedidas de hardware. El equipo de **PACAP** estudia los mecanismos de seguridad que inserta el compilador para mejorar la productividad del programador y la solidez de la aplicación frente a los ataques laterales.

2.10 Arquitectura de hardware, programación y compilación de bajo consumo

Como ya se ha mencionado en este libro, uno de los retos transversales más destacados es la eficiencia energética y, en general, la de los recursos. Muchos dispositivos IoT deben funcionar por años con una pequeña batería que no está previsto que se cambie ni se recargue. El reto consiste, por un lado, en dotar de mayor energía a los dispositivos IoT y, por otro, en reducir su consumo energético tanto desde el punto de vista del hardware como del software. Además, desde una perspectiva más global, se espera que los dispositivos IoT sean miles de millones. Incluso un pequeño descenso en el consumo individual de energía de miles de millones de aparatos permite ahorrar cantidades importantes de energía, abaratar los costos considerablemente y reducir el impacto medioambiental. Por lo tanto, hay que desarrollar una serie de líneas de investigación complementarias. A continuación detallamos algunas de ellas.

Impulsar la energía ultrabaja hacia la energía neta cero

El uso de cables o baterías para energizar los sistemas embebidos es un inconveniente por el factor de forma, precio o cuestiones de mantenimiento. Se debe seguir investigando en el diseño de dispositivos de comunicación autoenergizados, que no se alimentan ni de la batería ni de los cables, es decir, lo que aquí llamamos dispositivos IoT de uso de energía neta cero.

La identificación por radio frecuencia o RFID (por sus siglas en inglés) pasiva es un ejemplo en el que las etiquetas no tienen batería. Sólo se componen de un chip y una antena y se alimentan tras la lectura de datos realizada por un lector. Por lo tanto, esta tecnología es muy escalable desde el punto de vista energético, ya que un solo lector se puede utilizar para un número infinito de etiquetas. Sin embargo, las aplicaciones que la RFID pasiva permite son limitadas, ya que las

etiquetas no se pueden comunicar cuando no hay un lector cerca, y el lector suele consumir más energía que un simple dispositivo IoT (activo).

Algunas investigaciones se centran en el desarrollo de nuevos equipos IoT sin batería que cosechan la energía del entorno, por ejemplo, la luz, el calor, las vibraciones/movimientos o las ondas de radio. Sin embargo, estos procesos generan niveles de corriente demasiado bajos. Por lo tanto, los dispositivos de IoT de uso de energía neta cero se deben diseñar para que consuman la menor cantidad de energía posible.

Por ejemplo, las técnicas de bloqueo o gating de potencia permiten cortar la corriente a los bloques del circuito que no están en uso. Además, el uso de memorias no volátiles (NVM como la NVRAM) hace que, en teoría, un dispositivo pueda sufrir cortes de energía sin perder datos, lo que le permite continuar su tarea en lugar de reiniciarla. Las tecnologías actuales de NVM siguen presentando tiempos de escritura lentos, un alto consumo de energía de escritura y una duración de escritura limitada. Los retos de la investigación en este campo incluyen, por lo tanto, pensar en un nuevo hardware que capte mejor la energía del entorno y ofrezca mejores niveles de funcionamiento con el mínimo uso de corriente.

Un importante reto relacionado es el diseño de software y protocolos de red eficientes y robustos que funcionen en este tipo de hardware. En cuanto a la cadena de herramientas, uno de los retos es diseñar compiladores que puedan ayudar mejor a los programadores, mediante el análisis de los programas, en el contexto de la programación de dispositivos embebidos con alimentación de energía intermitente. Este análisis del programa se necesita para identificar estrategias eficientes de creación de puntos de restauración, también conocidos como check-pointing: qué estado del programa almacenar y cuándo.

↗ En Inria, el equipo-proyecto **PACAP** trabaja en compiladores y análisis de programas diseñados para facilitar el check-pointing en sistemas con alimentación intermitente.

Los aspectos de la arquitectura del software embebido plantean otra serie de dificultades.

Por ejemplo, sustituir ingenuamente la RAM tradicional por la NVRAM tiene efectos secundarios indeseables en el sistema embebido. Como las pérdidas de energía son frecuentes, se pueden producir en medio de la modificación de una estructura de datos no volátil. Cuando la plataforma se reinicia, el programa se reinicia con datos inconsistentes. Esta cuestión se conoce a veces como el problema

de la "máquina del tiempo rota". De hecho, a menos que todos los bits de todas las piezas de la memoria de un dispositivo (la CPU y la memoria, ¡pero también los dispositivos periféricos!) se hagan no volátiles, este problema puede ocurrir. Por lo tanto, todas las capas de software se ven afectadas por estas decisiones de arquitectura.

Los principales retos son:

- garantizar la coherencia de los datos y evitar una pérdida de rendimiento excesiva, con técnicas tanto en tiempo de ejecución como de compilación;
- diseñar un sistema multitarea eficiente en un contexto en el que se producen cortes de energía con frecuencia;
- diseñar protocolos de red que exploten la energía del entorno, evitando al mismo tiempo una pérdida de rendimiento excesiva cuando los nodos de la red se reinician con mucha frecuencia;
- proporcionar un servicio ininterrumpido ante la intermitencia de la conectividad de la IoT y/o la intermitencia de la energía.

Esquema de una placa experimental que incluye un microcontrolador con NVRAM. © *Inria / Photo C. Morel.*

↗ En Inria, el equipo-proyecto **SOCRAT**E trabaja en el diseño de arquitecturas robustas de software embebido para apoyar la recolección de energía y la energía intermitente en dispositivos IoT de energía neta cero.

↗ ZEP es un proyecto de investigación interdisciplinario iniciado por Inria que diseña diminutos dispositivos IoT inalámbricos y sin batería, que recogen la energía del entorno, basados en una novedosa arquitectura que incorpora una memoria de acceso aleatorio no volátil (NVRAM). Para beneficiarse de las innovaciones de hardware relacionadas con la recolección de energía y la NVRAM, y para optimizar el uso de la energía, ZEP diseña nuevos mecanismos de software, activos durante la compilación, por un lado, y durante la ejecución, por otro, que combinan aspectos de arquitectura, compilación y sistemas operativos.

Diseño de hardware IoT más rápido, más pequeño y más barato

Las posibilidades de escalamiento de la tecnología del hardware de la CPU están llegando a su límite. Posteriormente, la técnica más pertinente para aumentar la eficiencia energética (el número de cálculos por unidad de tiempo y por vatio consumido) es la especialización del hardware. Los aceleradores de hardware para dominios específicos pueden multiplicar la eficiencia energética por 100 (o más) en comparación con los computadores convencionales. Esta ganancia proviene principalmente de acercar los datos al cálculo y de eliminar el costo energético de la programabilidad total (búsqueda de instrucciones, caché, especulación, etc.). Los pequeños dispositivos embebidos también necesitan un hardware especializado para funcionar con limitaciones estrictas de potencia/energía. En los próximos diez años, esperamos que las especializaciones se vuelvan aún más habituales en respuesta a las cada vez mayores exigencias de rendimiento.

La gran demanda por impulsar/mantener más inteligencia en el borde de la red es un motor para una mayor eficiencia energética en los dispositivos IoT. Por ejemplo, los motores de aprendizaje automático e inferencia se ejecutan en la actualidad en un centro de datos remoto. En cambio, la próxima generación de redes neuronales se desplegará en el borde, para aprovechar los sensores en tiempo real que recogen los datos de entrenamiento y limitar el costo energético de transportar los datos brutos por la red. Por lo tanto, conviene diseñar aceleradores de hardware idóneos para redes neuronales en dispositivos IoT de bajo consumo.

Sin embargo, cuanto más especializado es el hardware, más difícil es de "programar". Los diseñadores de aceleradores de hardware para dispositivos IoT que funcionan en el rango de los milivatios (o menos) se deben enfrentar a una serie de obstáculos. Los diseñadores tienen que explorar un enorme espacio de diseño que abarque el hardware y el software. Los retos de investigación que se

plantean incluyen:

- identificar y definir las funcionalidades del stack de software de la IoT que se pueden acelerar, mientras que el resto se mantiene en los procesadores programables de bajo consumo;
- diseñar interfaces de programación relevantes para los aceleradores, lo que permite crear una frontera sin fisuras entre el software y el hardware;
- la reconfigurabilidad en tiempo de ejecución de los aceleradores sin que se pierda eficiencia;
- ofrecer un nivel suficiente de programabilidad en el acelerador (por ejemplo, definir el equivalente a la GPU de la IoT) para que se adapte a la evolución de los estándares o usos..

↗ En Inria, el equipo-proyecto **CAIRN** trabaja en el diseño de plataformas informáticas de hardware de muy bajo consumo para la IoT, especializadas pero programables, y nuevos niveles de abstracción para aceleradores de hardware de dominio específico. El equipo de **CAIRN** también trabaja en mejorar las arquitecturas de hardware de las CPUs embebidas con mecanismos que articulan la RAM no volátil y la energía intermitente.

Cómo habilitar los dispositivos IoT de escala milimétrica (polvo inteligente o smart dust)

Los recientes avances en microelectrónica han dado lugar a los primeros prototipos de micro-motes de un tamaño inferior al de un grano de arroz, que pueden detectar, computar y comunicarse sin componentes adicionales, en particular: sin necesidad de una placa de circuito impreso (PCB), y sin la unión de cables de varios chips. Esta miniaturización extrema es posible gracias a la eliminación de los osciladores de cristal externos, y depende únicamente de los circuitos osciladores internos a base de RC dentro del chip. Un micro-mote de este tipo puede ser muy pequeño y muy barato, lo que supone un emocionante avance tecnológico. Sin embargo, siguen existiendo importantes retos, que tienen que ver con el seguimiento preciso del tiempo en dichos dispositivos.

En particular, el inconveniente de utilizar un oscilador basado en RC es la deriva del reloj, que ronda las 16.000 ppm para un micro-mote sin cristal, frente a las 40 ppm de un oscilador de cristal. Las variaciones también dependen bastante de la temperatura. Un micro-mote sin cristal requiere una cuidadosa calibración manual de sus relojes para poder comunicarse con otros dispositivos disponibles. La ausencia de cristales en los micro-motes afectan la base misma de la

investigación inalámbrica de baja potencia. Prácticamente todas las plataformas inalámbricas de baja potencia están equipadas con una radio que se comunica de forma fiable y es capaz de medir el tiempo con precisión. La nueva disponibilidad de dispositivos IoT a escala milimétrica sin cristales abre, por ende, un ámbito de investigación y tiene el potencial de cambiar profundamente el campo de la investigación de baja potencia inalámbrica.

↗ En Inria, el equipo-proyecto **EVA** desarrolla algoritmos y protocolos de calibración que permiten que los dispositivos IoT a escala milimétrica se comuniquen con los dispositivos disponibles y formen redes coordinadas. En colaboración con UC Berkeley, **EVA** ha desarrollado SCuM, el primer micro-mote del mundo que cumple con los estándares de comunicación inalámbrica.

Domar el polimorfismo de hardware de bajo consumo

En el resto de la Internet, el hardware informático común ha confluido mayoritariamente en una configuración casi ubicua que combina procesadores de 64 bits (x86 o ARM).

En comparación, **la diversidad de hardware de IoT de bajo consumo es extrema.** Las arquitecturas de los procesadores que se encuentran varían enormemente, de una amplia variedad de proveedores, desde 8 a 16, 32 y 64 bits.

Esta diversidad de hardware tan extrema es un reto técnico en sí mismo: **la elección del hardware adecuado es difícil, y el desarrollo de software de IoT requiere con demasiada frecuencia conocimientos exóticos,** mientras que se exacerban los problemas de interoperabilidad.

La innovación en hardware de bajo consumo sigue apareciendo, a un ritmo que no disminuye. Un ejemplo reciente es la familia de arquitecturas de CPU extremadamente polimórficas, como RISC-V, que pondrá en jaque el statu quo y rivalizará con el creciente dominio de las CPU Cortex-M de ARM. En cuanto a las radios, surgen nuevas categorías de chips autoalimentados (sin pilas), que alterarán la noción misma de lo que es el bajo consumo. Al mismo tiempo, la miniaturización extrema promete soluciones de sistema en chip de próxima generación que equivaldrán esencialmente a polvo inteligente (“Smart Dust”), en cuanto a su tamaño.

Por ende, en un principio, el reto consiste en aprovechar esta extrema diversidad y, luego, **impulsar una evolución hacia menos de un puñado de plataformas de hardware de bajo consumo estándar y genéricas.**

Plataformas estándar de software embebido para hardware IoT de bajo consumo

Los requisitos de bajo consumo, ciberseguridad, interoperabilidad y funciones de gestión de dispositivos IoT aumentan considerablemente la complejidad del software IoT embebido, como también en los dispositivos de bajo consumo que se basan en microcontroladores. En el pasado, el software embebido en estos dispositivos ha tenido un único propósito, en su mayoría inmutable, propietario, y que dependía específicamente del hardware o del proveedor. Estas características están evolucionando a medida que aumenta la complejidad del software de la IoT. Ahora se espera que una gran parte de este software imite la dinámica típica del software de la era de Internet: más de uso general, de código abierto, reutilizable entre hardware y proveedores heterogéneos, y que aplique un conjunto de normas y API comunes. Se ha hecho necesario fomentar el software genérico de IoT en todos los sectores industriales (por ejemplo, mismo algoritmo de control, misma implementación, aplicada a diferentes industrias). Esta evolución ha propiciado la aparición de una gran cantidad de diversos sistemas operativos embebidos que aspiran a proporcionar una plataforma de software adecuada. Muchos vendedores y actores de las grandes tecnologías impulsan sus propias plataformas, y destacan que estas son cruciales, y que se espera una consolidación del mercado. El reto de estas plataformas de software profundamente embebidos es equilibrar el rendimiento (energía y latencia ultrabajas, huella de memoria diminuta, entre otros) con las garantías de seguridad y protección, a la vez que se facilita el desarrollo/portabilidad del código profundamente embebido en un hardware de IoT extremadamente diverso y de bajo consumo.

↗ En Inria, los equipos de los proyectos tales como **TRIBE** y **EVA** trabajan en el diseño de plataformas de software IoT embebidas, compactas y de bajo consumo. Por ejemplo, el sistema operativo RIOT. Otro ejemplo es OpenWSN, el stack de red 6TiSCH de código abierto de referencia.

↗ RIOT es un sistema operativo de uso general, independiente del proveedor, para pequeños dispositivos IoT que no pueden utilizar Linux debido a las limitaciones de recursos de su hardware. RIOT ofrece una plataforma gratuita y de código abierto, desarrollada por una gran comunidad que reúne a empresas, académicos y aficionados, repartidos por todo el mundo, cofundada por Inria. El objetivo de esta plataforma es implantar y agrupar los elementos necesarios para una Internet de las Cosas más duradera, segura, transparente y que respete la privacidad.

2.11 Optimización de la huella de recursos globales

Por un lado, el rendimiento tiene múltiples facetas, como la velocidad, la precisión, las garantías de seguridad, la equidad, etc. Por otro lado, hay que evaluar el rendimiento no sólo a nivel local, sino también en el contexto más amplio del sistema global. Ante las estrictas limitaciones de frugalidad de recursos, hay que explorar nuevas compensaciones en los dispositivos de la IoT a nivel local. A nivel más general, frente a una crisis ecológica global, se necesita una evaluación completa de la relación huella/beneficios de la IoT.

Aprovechamiento de los nuevos compromisos entre rendimiento y energías

La mayor parte de la computación actual se lleva a cabo con un sobreaprovisionamiento importante en términos de calidad del resultado (por ejemplo, en cuanto a precisión). Sin embargo, muchas veces se pueden obtener resultados aceptables a partir de cálculos inexactos o aproximados. Tanto las aplicaciones tradicionales (señal, imagen, visión, comunicaciones inalámbricas, etc.), como las emergentes (aprendizaje automático, minería de datos, etc.) exhiben una resiliencia intrínseca a los errores. Por lo tanto, un menor rendimiento a cambio de un menor consumo de energía es un compromiso habitual que hay que revisar en el contexto de la IoT.

Por ejemplo, el aprovechamiento del compromiso entre energía y precisión (manteniendo la funcionalidad dentro de límites aceptables) es un enfoque prometedor para mejorar la eficiencia energética, complementario a la aceleración por hardware. Por ejemplo, se puede obtener una ganancia de más de 50 veces en eficiencia energética si se cambia una operación de baja precisión de 8 bits, adecuada para la visión, por una operación de doble precisión en coma flotante de 64 bits, que se necesita para los cálculos científicos de alta precisión (teniendo en cuenta el almacenamiento, el transporte y el cálculo de los datos). Hasta ahora, las optimizaciones se han centrado principalmente en las representaciones de bajo nivel del cálculo aritmético, que no se adaptan a las grandes aplicaciones de la IoT. Del mismo modo, se pueden obtener enormes ganancias cuantificando severamente los pesos de un modelo de aprendizaje automático, para que se

ajusten a la diminuta memoria y a las pequeñas capacidades de la CPU disponibles en un dispositivo IoT de bajo consumo.

El reto consiste ahora en diseñar niveles de abstracción más altos que mejoren la escalabilidad y en identificar las transformaciones de alto nivel que afectan a la precisión. La aceptabilidad de la aproximación se basa en el conocimiento específico del dominio, que se debe actualizar (puede evolucionar) y aprovechar de forma eficiente. El programador puede ajustar el grado de aproximación durante el diseño o la ejecución. En este sentido, constituye un desafío la integración del análisis y las transformaciones del compilador (por ejemplo, la identificación de regiones prometedoras, la descomposición jerárquica de grandes programas y las transformaciones algorítmicas) en el ajuste de la precisión.

A partir de principios similares, los retos de investigación relacionados incluyen la exploración de otros compromisos, como por ejemplo la velocidad frente al consumo de energía, o el aumento de la seguridad frente al menor consumo de energía.

↗ En Inria, el equipo-proyecto **CAIRN** estudia los compromisos (trade-offs) entre precisión y energía, el diseño de métodos para optimizar las arquitecturas informáticas de baja precisión específicas del dominio para la IoT, y la inferencia/entrenamiento para redes neuronales profundas en el borde de la red. El equipo-proyecto **TRIBE** estudia los compromisos en términos de costos de comunicación y computación, así como la precisión y la privacidad, con enfoques de modelos de aprendizaje automático jerárquico, cuyo objetivo es dividir y distribuir la inferencia a lo largo del continuo de la IoT: desde el dispositivo restringido hasta la nube, pasando por el borde.

Los dispositivos IoT consumen energía no sólo para detectar, computar y procesar datos, sino también para comunicarse a través de la red. Por lo tanto, un enfoque que siempre resulta prometedor en cuanto a la reducción del consumo de energía es la reducción de la frecuencia y el tamaño de las transmisiones de datos. No obstante, el envío de una menor cantidad de datos podría disminuir la precisión de los datos disponibles a distancia. Por lo tanto, existe un compromiso entre la precisión de los datos y la reducción de la comunicación.

Un área interesante de investigación en este ámbito es el diseño de mecanismos de doble predicción, en los que se utilizan técnicas de aprendizaje automático para inferir la siguiente transmisión de datos basándose en las transmisiones de datos anteriores. Los nuevos datos se transmiten sólo si la predicción difiere demasiado de los nuevos datos. El reto consiste en adaptar los motores y modelos

de aprendizaje automático a los muy reducidos presupuestos de recursos (memoria/computación) disponibles en los dispositivos IoT

Servicio ininterrumpido con conectividad o alimentación intermitente

IPara reducir el consumo global de los dispositivos IoT, se está investigando el stack de comunicaciones para establecer ciclos de trabajo de manera que cada nodo pueda apagar su interfaz o interfaces de comunicación regularmente. Entonces se dice que el nodo está en reposo. De hecho, la comunicación es la tarea que más energía consume para un nodo IoT (comparado con la detección y el procesamiento). Pero cuando la interfaz de comunicación está en reposo, el nodo está desconectado y no puede recibir mensajes. Si se envía un mensaje a un nodo en reposo, el mensaje se perderá y se desperdiciará la energía que se ha gastado para enviarlo. En un sistema IoT tradicional, se pueden aplicar varios mecanismos para anunciar a un nodo cuando se despierta que debe permanecer despierto. El sistema podría estar completamente sincronizado y así los nodos saben cuándo deben despertarse y escuchar, y cuándo pueden ponerse en reposo. (¡Y conseguir una sincronización precisa en redes muy distribuidas es todo un reto!) Pero en las redes asíncronas (como la mayoría de las redes IoT), el emisor tiene que enviar generalmente una breve señal o los datos completos con regularidad hasta que el receptor se despierta, recibe la señal o los datos, y reconoce al emisor.

El hardware de los dispositivos IoT suele ofrecer modos de ahorro de energía agresivos (modos de suspensión) que consumen una energía insignificante, pero requieren la desactivación temporal de la CPU y las interfaces de red. Sin embargo, para que la comunicación en red sea exitosa se necesita que el emisor y el receptor estén activos simultáneamente. Parece haber un compromiso para permitir que cada dispositivo duerma lo máximo posible, pero activándose en los momentos adecuados para garantizar la funcionalidad global.

Las redes síncronas de IoT resuelven este problema programando por adelantado cuándo se despiertan y escuchan los dispositivos, y cuándo se ponen en reposo. Un desafío difícil en este contexto es diseñar mecanismos de programación inteligente y sincronización precisa, con menos sobrecarga, en redes altamente distribuidas.

Las redes asíncronas de IoT (el grueso de IoT hasta ahora) plantean diferentes retos que hay que abordar. En este ámbito, un área activa de investigación es el diseño de “wake-up radio” o radio despertador, en el que los dispositivos están

equipados con interfaces de radio duales. La interfaz principal, que se utiliza para la transferencia de datos, está desactivada por defecto. Se utiliza una interfaz secundaria de muy bajo consumo para recibir señales de activación. Se están investigando los receptores pasivos de activación, cuyo reto es aumentar su sensibilidad sin aumentar la potencia de transmisión.

Un enfoque complementario es el almacenamiento en caché de datos, en nombre de los nodos durmientes, en algún lugar del continuo Nube-Edge-Cosa. El reto consiste en determinar y evaluar estrategias novedosas de almacenamiento y sustitución de caché que:

- optimice dónde almacenar los datos de la IoT: el costo se reduce cuando se está más cercano al solicitante, pero esto podría estar lejos de la fuente de los datos;
- optimice el número de duplicados a almacenar: las ubicaciones múltiples aumentan el costo que supone almacenar los datos, pero pueden reducir el costo de recuperarlos, ya que es más probable que estén más cerca del solicitante;
- optimice la frecuencia de las actualizaciones: un mayor número de actualizaciones mejora la precisión pero aumenta el costo.

Evaluar y minimizar la huella global de la IoT

La actual crisis ecológica urge a los investigadores de todos los campos a evaluar el impacto medioambiental de las diferentes tecnologías en uso actuales o futuras. Entre otras cosas, la IoT permite una mejor clasificación y reciclaje de los residuos, una iluminación de las calles más respetuosa con el medio ambiente o una mejor gestión del tráfico vial. De este modo, la IoT puede ayudar a reducir nuestro impacto en el medio ambiente de muchas maneras, tal y como afirman varios estudios[4 5 6].

Aun así, la investigación se suele centrar demasiado en alguna optimización potencial que podría proporcionar una tecnología de la IoT, y pasa por alto un análisis exhaustivo que evalúe las condiciones en las que las ganancias netas podrían producirse realmente, y si es probable que estas condiciones se cumplan o no.

Se debe evaluar el impacto medioambiental directo, teniendo en cuenta todo el ciclo de vida de los dispositivos, desde su producción (por ejemplo, la extracción de recursos minerales), pasando por sus gastos de funcionamiento (por ejemplo, el mantenimiento y el consumo de energía), hasta el final de su vida útil (por ejemplo, su posible reciclaje). Aquí, la mejora de la reciclabilidad de los pequeños

4. 5 ways the IoT is helping the Environment.
5. Where IoT Meets The Environment: Building a Greener Future.
6. IoT for Environmental Sustainability.

componentes electrónicos de la IoT supone un gran reto para la investigación.

Todos los dispositivos IoT están hechos de componentes electrónicos. Por lo tanto, un reto fundamental es construir y diseñar hardware utilizando menos recursos. Por ejemplo, algunas investigaciones se centran en la miniaturización de la placa de circuito impreso (PCB), por ejemplo para utilizar menos metal y plásticos, o en permitir el uso de nuevos materiales prometedores como el grafeno.

También hay que afrontar los retos de la investigación en el diseño de antenas (que a veces pueden imprimirse con tinta biodegradable [7]) y de baterías más respetuosas con los recursos.

Además, se debe evaluar el impacto indirecto, que abarca los efectos inducidos, los efectos de rebote, etc., ya que es probable que los nuevos usos contrarresten las optimizaciones permitidas por la IoT. Por ejemplo, los trillones de dispositivos inalámbricos microscópicos sin batería que se alimentan de la recolección de energía, aunque se aprovechen para los servicios avanzados de la próxima generación de Internet, pueden seguir provocando, a nivel mundial, más emisiones de gases de efecto invernadero.

Normalmente, la investigación se centra en la mejora del impacto directo potencial, pero no llega a responder a preguntas más globales: ¿en qué medida se mejora en la práctica? ¿Hasta cuándo? ¿A qué costo? Y sobre todo, ¿cuáles son los beneficios netos a nivel global? En este campo, la complejidad aumenta porque se requieren competencias extremadamente interdisciplinarias, que combinan no sólo conocimientos tecnológicos, sino también sociales, económicos y políticos.

Un reto que se plantea en este ámbito es, el diseño de marcos conceptuales adecuados que puedan captar y evaluar mejor todo el espectro del impacto medioambiental de la IoT. Los marcos actuales no suelen captar el impacto indirecto, aunque éste puede ser mucho mayor que el impacto directo. Aunque teóricamente el impacto directo se puede captar con los marcos existentes, éstos se ven dificultados porque (i) es difícil reunir datos y (ii) la tecnología y los usos cambian a un ritmo vertiginoso.

7. D. Iba, et al. "Development of smart gear system by conductive-ink print," Proc. SPIE, 2019.

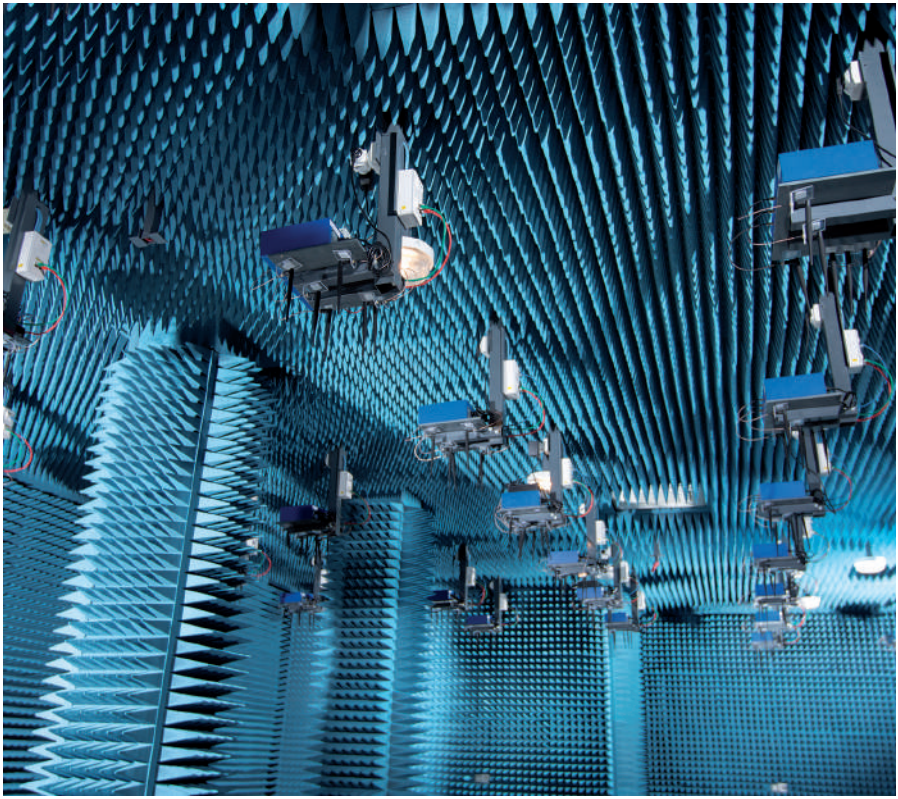
Conclusión

La Internet de las Cosas ha adquirido una importancia fundamental en el panorama de las tecnologías que darán forma al mañana. En el mundo que se avecina, las entidades (países, organizaciones, empresas, individuos) que pretendan preservar su soberanía deben tomar conciencia y dedicar los medios necesarios para liderar actividades de investigación sustanciales y de desarrollo tecnológico profundo, en varios dominios que subyacen a la IoT.

Estos ámbitos son diversos y abarcan desde las redes de comunicación de nueva generación hasta la informática distribuida, desde el software de los sistemas embebidos hasta el hardware de bajo consumo, desde la interacción hombre-máquina hasta el control y la resistencia de los sistemas ciberfísicos, desde la ciberseguridad y la protección hasta el procesamiento de datos para preservar la privacidad.

Además, a medida que la tecnología de la IoT se entrelaza más estrechamente con la sociedad y nuestras vidas personales, la creación de normas para la tecnología IoT resulta cada vez más importante. En este contexto, para estar en condiciones de preservar la neutralidad geopolítica de la tecnología IoT, la participación activa en las organizaciones de desarrollo de normas pertinentes resulta crucial.

Por último, pero no por ello menos importante, a medida que aumenta la crisis medioambiental, existe la esperanza de que nuestro impacto en la naturaleza se pueda reducir gracias a más mecanismos potenciados por la IoT, que se desplegarán y utilizarán de forma masiva. No obstante, se necesitan grandes esfuerzos complementarios para evaluar si esta reducción compensará globalmente el impacto medioambiental de la producción, el despliegue y el mantenimiento de estos mecanismos de la IoT, en todo su ciclo de vida.



Sala anecoica de la plataforma experimental FIT (Future Internet of Things). © Inria / Photo C. Morel.

Notas

Domaine de Voluceau, Rocquencourt BP 105
78153 Le Chesnay Cedex, France
Tel.: +33 (0)1 39 63 55 11
www.inria.fr