UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

Design and Validation of Novel Secure Protocols for Internet of Things leveraging on Low-power Communication Technologies

Diseño y Validación de Nuevos Protocolos Seguros para Redes de Internet de las Cosas basadas en Tecnología de Comunicación de Bajo Consumo

D. Jesús Sánchez Gómez

2021

Universidad de Murcia

Facultad de Informática

Diseño y Validación de Nuevos Protocolos Seguros para Redes de Internet de las Cosas basadas en Tecnología de Comunicación de Bajo Consumo.

Tesis Doctoral

Presentada por:
Jesús Sánchez Gómez

Supervisada por:
Dr. Miguel Ángel Zamora Izquierdo
Dr. Rafael Marín Pérez

Murcia, Octubre de 2021

University of Murcia

Faculty of Computer Science

Design and Validation of Novel Secure Protocols for Internet of Things leveraging on Low-power Communication Technologies

Ph.D. Thesis

Authored by:
Jesús Sánchez Gómez

Supervised by:
Dr. Miguel Ángel Zamora Izquierdo
Dr. Rafael Marín Pérez

Murcia, October 2021

A mi madre.

Agradecimientos

Primero me gustaría agradecer a la Fundación Séneca y a Odin Solutions por haber ofrecido la financiación y el apoyo que han permitido la realización de este proyecto de tesis. Así como al Departamento de Ingeniería de la Información y las Comunicaciones por acogerme.

A todos los compañeros con los que he tenido la oportunidad de colaborar durante estos últimos años.

Por último, pero no por ello menos importante, le doy mi más sincero agradecimiento a mis directores y tutor, Miguel Ángel, Rafa y Antonio, por haberme dado la oportunidad de dedicarme a este oficio, y por su paciencia infinita conmigo.

Sin la ayuda de todas estas personas brillantes y trabajadoras, esta tesis no habría sido posible.

"DON'T PANIC". The Hitchhiker's Guide to the Galaxy.

Contents

List of Figures

List of Tables

Abbreviations

3GPP	The 3rd Generation Partnership Project
5G-CN	The Core Network
5GPPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorization, and Accounting
ACE	IETF's Authorization for Constrained Environments Work Group
ACE-OAuth	Authorization for Constrained Environments using the OAuth 2.0 Framework
AWS	Amazon Web Services
BoF	Birth of Feathers
CBOR	Concise Binary Object Representation
COSE	CBOR Object Signing and Encryption
CSS	Chirp Spread Spectrum
CoAP	Constrained Application Protocol
CoAP-EAP	EAP-Based Authentication Service over CoAP
DDoS	Distributed Denial-of-Service
DTLS	Datagram Transport Layer Security
DVB	Digital Video Broadcasting
DoS	Denial-of-Service
EAP	Extensible Authentication Protocol
EAP-AKA'	Improved EAP Authentication and Key Agreement
EAP-PSK	Pre-Shared Key EAP method
ECC	Elliptic Curve Cryptography
EDHOC	Ephemeral Diffie-Hellman Over COSE
eDRX	extended Discontinuous Reception
eMBB	enhanced Mobile Broadband
ENISA	European Union Agency for Cybersecurity
ESA	European Space Agency
ETSI	European Telecommunications Standards Institute
FOTA	Firmware Over the Air
HSS	Home Subscriber Server
ID	IETF Internet Draft
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange Protocol Version 2
IMT-2020	The International Mobile Telecommunications-2020
ISM	Industrial, Scientific and Medical band
IoT	Internet of Things
JSON	JavaScript Object Notation
LO-CoAP-EAP	Low-Overhead CoAP-EAP
LPWAN	Low-Power Wide-Area Network
LR-WPAN	Low-Rate Wireless Personal Area Network

LTE-M	Long Term Evolution for Machines
LwM2M	Lightweight M2M standard
MCU SoC	Microcontroller System-on-Chip
MEC	Multi-access Edge Computing
MEF	Metro Ethernet Forum
ML	Machine Learning
mMTC	massive Machine Type Communications
MSK	Master Session Key
MTU	Maximum Transmission Unit
MitM	Man-in-the-Middle
N3IWF	Non-3GPP InterWorking Function
NAS	Non-Access Stratum
NB-IoT	Narrowband-IoT
NFC	Near Field Communication
NGMN	Next Generation Mobile Networks Alliance
NIS	Network and Information Security
OMAC	One-key Message Authentication Checksum
ONF	Open Network Foundation
OSCORE	Object Security for Constrained RESTful Environments
PANA	Protocol for Carrying Authentication for Network Access
PDU	Protocol Data Unit
QoS	Quality-of-Service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RoHC	Robust Header Compression
SCADA	Supervisory Control And Data Acquisition
SCHC	Static Context Header Compression
SFM	Session Management Function
SoC	System-on-Chip
TSK	Transient Session Key
UE	Mobile User Equipment
ULI	User Location Info
UPF	User Plane Function
URI	Unique Resource Identifier
URLLC	Ultra-Reliable and Low-Latency Communications
USIM	Universal Subscriber Identity Module
WG	IETF Work Group
WSN	Wireless Sensor Network

Capítulo 1

Resumen

1.1. Motivación

El Internet de las Cosas (*Internet of Things*, IoT) es un término que fue acuñado por primera vez en 1999 [1] refiriéndose a la intercomunicación de chips RFID sobre Internet. Sin embargo, a día de hoy, el IoT representa un concepto más amplio y de mayor nivel. IoT introduce un paradigma que expande el alcance de Internet más allá de los recursos digitales, mediante el acceso y control remoto a recursos físico a través de protocolos de comunicación basados en IP [2]. Históricamente, avances significativos en redes de computadores han sido siempre orientados hacia las centradas en la interacción con humanos, donde un humano es tanto el principal productor como consumidor de la información que circula por Internet. Por esta razón, alcanzar una mejor experiencia de Internet centrada en la interacción de humanos mediante un mayor ancho de banda o una menor latencia para el acceso a recursos digitales era una de las principales metas tanto de la industria como de la academia. Pero el IoT considera que las máquinas producen y consumen una cantidad creciente de datos si los comparamos con las interacciones con humanos.

El IoT ha impactado severamente tanto las actividades sociales como industriales. Previamente, las distintas soluciones comerciales y productos incluían el paradigma IoT como un añadido, una vez el objetivo había sido alcanzado. Pero, en años recientes, el paradigma IoT es ahora una parte del diseño en sí mismo, considerado incluso antes de que el plan de negocio sea elaborado. El volumen de ingresos de las actividades relacionadas con el IoT está en continuo crecimiento [3], [4]. Se estima que 18 miles de millones de dispositivos estarán conectados a Inernet en 20222 [5]. Además, como la definición de lo que es o no un dispositivo IoT varia entre diferentes instituciones, los valores estimados pueden cambiar en diferentes informes. La Figura 1.1 muestra el crecimiento de dispositivos IoT conectado en otro informe, el cuál establece que habrán más de 25 miles de millones de dispositivos IoT conectados para 2030 [6]. También, se espera que el mercado IoT alcance un valor estimado de USD1.567 billones para 2025 [7]. Como consecuencia, el IoT se ha convertido en un tema de interés tanto para la industria como academia, afectando la mayoría de tejidos productivos en escenarios diversos. En esencia, el IoT crea valor mediante la conexión de dispositivos midiendo y actuando sobre el medio físico en el que se encuentran, de un modo cooperativo. Esto permite, no sólo el control y monitorización remotos, si no también acumular valiosos datos estadísticos, que pueden ser analizados para la obtención de conocimiento especializado y la resolución de problemas complejos de un modo sin precedentes. Algunos ejemplos de aplicación incluyen Ciudades Inteligentes (Smart Cities), Industria

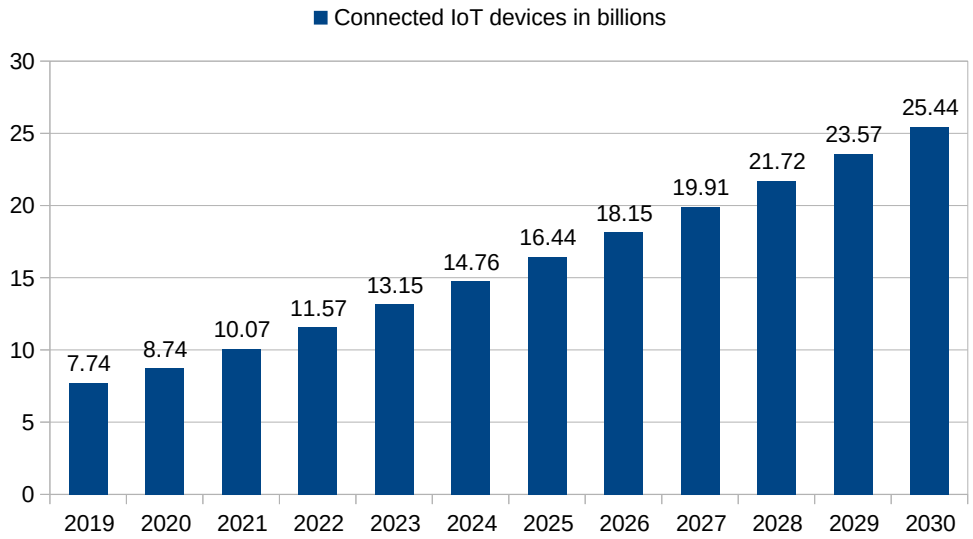

Figura 1.1: Previsión de miles de millones de dispositivos IoT conectados. Fuente [6]

4.0, Agricultura Inteligente (Smart Agriculture), Cibermedicina (e-Health) y Sistemas de Transporte Inteligente (Intelligent Transportation Systems).

Anterior a la popularización del IoT, diferentes verticales ya utilizaban las tecnologías de la información para la monitorización y control remotos. Estas aprovechaban hardware embebido que está conectado a diversos sensores y actuadores electro-mecánicos, enviando datos de vuelta hacia los componentes centralizados. Los administradores de despliegues tienen acceso a una plataforma amigable para humanos mediante el que acceder al estado actual del sistema completo, mediante lo que es conocido como una plataforma *Supervisory Control And Data Acquisition* (SCADA). La infraestructura posicionada en el último kilómetro que soporta las tareas de control y monitorización remotas es conocido como Redes de Sensores Inalámbricas (*Wireless Sensor Networks*, WSNs). Éstas son incluso anteriores al paradigma IoT y han sido implementadas en una gran variedad de tecnologías específicos de fabricante que implementan soluciones ad-hoc para los problemas de comunicación y seguridad, diseñadas alrededor de las limitaciones del dispositivo final y la tecnología radio. Lo que separa el IoT de las WSNs es un nivel predominantemente mayor de compatibilidad. Esto es conseguido a través del uso de protocolos basados en Internet en la capa de red. Así, despliegues pertenecientes a diferentes dominios administrativos o que utilizan soluciones específicas por fabricante, son capaces de interoperar a través de redes basadas en IP.

Gracias a sus beneficios, la industria IoT motiva la aparición de productos y servicios en el mercado para diferentes áreas de aplicación. Por este motivo, los dispositivos componen un entorno diverso y heterogéneo, realizando un amplio rango de funcionalidades. Estas van desde la inclusión de una lógica de operación muy específica, como una bombilla controlada remotamente, hasta un dispositivo más genérico, como un teléfono móvil inteligente. Adicionalmente, los dispositivos IoT tienen un amplio rango de características computacionales, que van desde dispositivos embebidos basados en microcontroladoras, hasta aplicaciones corriendo en hardware común. También, la naturaleza del ancho de banda requerido varía ampliamente, yendo desde dispositivos que permanecen la mayor parte del tiempo en un estado de letargo y envían pequeños mensajes periódicamente, hasta dispositivos que realizan tareas críticas y requiere de un canal de comunicación con ultra-baja latencia y un gran ancho de banda. Como consecuencia, uno de los mayores retos asociados a los escenarios IoT es proveer soluciones de ingeniería que empleen un conjunto de protocolos o tecnologías hechas a medida para las características de los dispositivos utilizados en su red.

Existe un subconjunto de aplicaciones que ha sido especialmente beneficiado de las tecnologías de control y actuación remota. Estos escenarios incluyen Smart Cities, Industry 4.0 y Smart Agriculture,

entre otros. Son soportados por dispositivos embebidos sensores y actuadores esparcidos en una gran área geográfica, trabajando típicamente sin supervisión humana, prescindiendo de acceso a una red eléctrica y fuera del rango de redes celulares. Los requisitos específicos encontrados en estos escenarios presentan un gran conjunto de retos y brechas para las actuales tecnologías de comunicación IoT. Un paradigma novedoso para cubrir esta brecha son las Redes de bajo consumo y largo alcance (Low-Power Wide-Area Networks, LPWANs) [8]-[14]. Reducen el coste por dispositivo mediante el uso de tecnologías radio de largo alance y bajo consumo que son capaces de cubrir una gran área con menor cantidad de estaciones bases, las cuáles a su vez soportan un mayor número de dispositivos por celda. Sin embargo, las LPWANs tienen un severamente limitado canal de comunicación, diseñado para soportar transmisiones cortas y esporádicas, a relativamente bajas tasas de datos — en el orden de bps or kbps. Consecuentemente, otra brecha importante encontrada en los escenarios basados en LPWANs es la seguridad y la privacidad, dada su preferencia por soluciones simples diseñadas por el fabricante para reducir la sobrecarga de cabeceras. Por este motivo, las tecnologías comunes utilizadas en seguridad y privacidad para Internet no son practicables en redes limitadas, debido a su prohibitivo gran tamaño de cabeceras y número de transmisiones requerido. Por lo tanto, las LPWANs han resultado en islas de comunicación aisladas y específicas del fabricante, que impiden la interoperabilidad segura y privada de dispositivos embebidos a través de Internet. Esto contradice la propia esencia del paradigma IoT, el cuál se basa en el uso de protocolos estandarizado de Internet abiertos para fomentar un entorno cohesivo e interoperable, donde diferentes entidades colaboran compartiendo información acerca de su entorno, resolviendo poroblemas difíciles.

Esta tesis doctoral describe los resultados de investigación obtenidos del diseño, implementación y validación de protocolos seguros y novedosos para IoT, basados en tecnologías de la comunicación de bajo consumo. Estos protocolos permiten la comunicación segura de dispositivos embebidos con Internet sobre tecnologías LPWAN, adaptándose a cada caso de uso y características del despliegue. La comunicación interoperable de dispositivos finales sobre Internet se proveen a través del mecanismo *Static Context Header Compression (SCHC)*, definido en la RFC8724 [15]. Este mecanismo soporta la comunicación interoperable de dispositivos pertenecientes a diferentes dominios administrativos y utilizando diferentes tipos de LPWAN. Esto permite que una variedad heterogénea de dispositivos alimentados por batería sean desplegados sobre tecnologías como Sigfox [16], LoRaWAN [17], Narrowband-IoT (NB-IoT) [18]-[22] o Long Term Evolution for Machines (LTE-M) [10]. Para proveer de seguridad y privacidad a la comunicación, así como también de una solución de gestión legible para humanos para despliegues masivos y heterogéneos, estos dispositivos realizan un proceso de autenticación y compartición de claves basado en el marco *Authentication, Authorization, and Accounting* (AAA) [23], [24]. Tras la evaluación de diferentes capas de aplicación, estas contribuciones están alineadas con el uso de Constrained Application Protocol (CoAP) [25], considerado por la *Internet Engineering Task Force* (IETF) como uno de los bloques básicos para el futuro de los entornos limitados, permitiendo un acceso a los recursos basado en interacciones web de solicitud y respuesta en escenarios con redes tolerantes al retardo y la pérdida de datos [26].

Esta tesis doctoral ha sido financiada por la Fundación Séneca[1], Comunidad Autonóma de la Región de Murcia (España) a través del programa FPI con Referencia No. 20751/FPI/18 y cofinanciado por Odin Solutions S.L.[2]

1.2. Objetivos y Metodología

El conjunto de retos y brechas previamente mencionado en comunicaciones actuales de IoT para entornos de bajo consumo ha propiciado el desarrollo y contribuciones contenidas en esta tesis. La intención es establecer las bases para redes de sensores y actuadores de bajo consumo que requiere acceso seguro e interoperable a despliegues de terceros a través de una red basada en protocolos de Internet. La metodología fue elaborada mediante la combinación de problemas de ingeniería de

[1] http://fseneca.es/
[2] https://www.odins.es/en

red sobre la transmisión eficiente de paquetes basados en IP sobre redes de bajo consumo. En una segunda parte, la metodología se centra en problemas de diseño e implementación asociados a establecer un despliegue seguro, privado e interoperable sobre redes de bajo consumo, siguiendo el principio fundamental del paradigma IoT de utilizar Internet como una base común. Después, ambas partes han sido unidas para alcanzar la interoperabilidad eficiente de dispositivos limitados sobre redes de bajo consumo a través de Internet en una forma segura y privada. A través del desarrollo de esta tesis, sus diferentes contribuciones fueron integradas en los resultados de proyectos financiados por la Unión Europea dentro del programa H2020, como Fed4IoT[3], CYSEMA[4] y el proyecto H2020 *open call* IoTrust[5]. Finalmente la propuesta de investigación ha sido validada utilizando tecnologías LPWAN sobre sendos despliegues basados en bandas de radio licenciadas y no licenciadas. Así, los objetivos de investigación de esta tesis son los siguientes:

- Objetivo 1: Estudiar la viabilidad y requisitos de dispositivos embebidos transmitiendo sobre LPWAN de forma segura usando protocolos basados en IP.
- Objetivo 2: Analizar las soluciones del estado del arte para integrar de forma segura LPWANs de terceros dentro de sistemas celulares 4G y 5G.
- Objetivo 3: Estudiar y analizar mecanismos de compresión de cabeceras y fragmentación para la transmisión de paquetes basados en tecnologías de Internet sobre tecnologías de comunicación de bajo consumo.
- Objetivo 4: Estudiar y analizar mecanismos ligeros para autenticación y compartición de claves para entornos limitados.
- Objetivo 5: Implementar un mecanismo eficiente de compresión de cabeceras y fragmentación para la transmisión de paquetes basados en protocolos IP sobre tecnologías de comunicación de bajo consumo.
- Objetivo 6: Implementar un mecanismo ligero de autenticación y compartición de claves para entornos limitados, centrado en la interacción humana.
- Objetivo 7: Integrar y validar en hardware real un mecanismo eficiente de compresión y fragmentación para la transmisión de paquetes IP sobre tecnologías de comunicación de bajo consumo.
- Objetivo 8: Integrar y validar en hardware real la comunicación autenticada y segura de dispositivos sobre LPWAN.

El proceso seguido para alcanzar estos objetivos ha consistido en establecer sublíneas de investigación asociadas a cada uno de los objetivos, que convergen finalmente como un todo para componer esta tesis. Todos estos objetivos son abordados repetidas veces, siguiendo una metodología incremental e iterativa. Cada una de las pasadas produce como resultado nuevo conocimiento en un lazo cerrado de retroalimentación que mejora y refina la siguiente iteración. Las diferentes fases incluyen análisis de requisitos, investigación del estado del arte, diseño de la propuesta, evaluación y validación. Siguiendo esta metodología mejora los resultados conseguidos por cada uno de los objetivos y da forma a la contribución final.

En este sentido, para conseguir un estudio de los requisitos computacionales y de comunicación de entornos limitados, un escenario real fue desplegado con dispositivos embebidos y una infraestructura radio para alcanzar un escenario LPWAN que use tanto tecnologías basadas en bandas de radio no licenciadas como licenciadas, consistiendo en LoRaWAN y NB-IoT, respectivamente. Después, un análisis de las alternativas del estado del arte fue realizado para la integración de tecnologías IoT de bajo consumo de terceros en redes celulares, particularmente en el sistema 5G. Luego, los requisitos de

[3] https://fed4iot.org/
[4] https://www.iot4industry.eu/project_cysema
[5] https://www.odins.es/en/iot-trust-security-on-internet-of-things/

Tabla 1.1: Principales resultados de la tesis

Resultado	Objetivos	Publicación
R1. Análisis de los requisitos para que dispositivos embebidos transmitan de forma segura paquetes basados en protocolos IP y análisis de las deficiencias en las soluciones actuales para la integración de tecnologías LPWAN en el paradigma IoT.	1,2	[119] [120] [121] [122] [123]
R2. Análisis de las soluciones en el estado del arte para integrar LPWANs de terceros en redes celulares.	1,2,3	[119] [121] [123] [124]
R3. Implementar un mecanismo ligero de autenticación y compartición de claves para entornos limitados a través de técnicas y herramientas viables para este paradigma y así abordar una gestión administrativa escalable para despliegues IoT heterogéneos.	4,6	[119] [121] [124] [125] [126] [127]
R4. Implementar un mecanismo de compresión de cabeceras IPv6/UDP/CoAP y fragmentación basado en los esfuerzos de estandarización de la IETF para integrar entornos limitados con Internet.	3,5	[120] [125] [126] [127]
R5. Validación y evaluación de las soluciones propuestas en escenarios reales para poder verificar su viabilidad.	5,6,7,8	[120] [121] [127]

transmisión de paquetes IPv6/UDP sobre LPWANs fueron estudiados. Como consecuencia, diferentes alternativas para la compresión de cabeceras y fragmentación fueron analizados. Esto llevó al diseño, implementación y validación de un mecanismo de compresión de cabeceras y fragmentación de paquetes IPv6/UDP/CoAP basado en la estandarización de la IETF, para la integración de dispositivos limitados en Internet — SCHC. Finalmente, la integración de diferentes mecanismos de seguridad y privacidad basados en tecnologías Internet dentro del ecosistema limitado fue analizada. Esto llevó al diseño, implementación y validación de una técnica ligera de autenticación y compartición de claves basada en la infrastructure AAA, utilizando la pila de protocolos IP sobre redes tolerantes al retardo y a las pérdidas de datos.

1.3. Resultados

Las contribuciones de los objetivos de esta tesis doctoral anteriormente descritos, han derivado en diferentes publicaciones científicas en revistas y conferencias de ámbito internacional, tal y como se muestra al final del Capítulo 5. Los resultados clave se muestran en la Tabla 1.1, dispuestos junto a los objetivos abordados. Es más, el trabajo desarrollado durante la tesis ha sido empleado en diferentes proyectos fundados por la Unión Europea, tal y como se describe en la Sección 1.2. Además, se ha extendido la discusión de los esfuerzos de estandarización de la IETF para integrar dispositivos embebidos en el ecosistema de Internet, especialmente por los IETF's LPWAN and ACE *work groups*. Nótese que esta tesis ha sido presentada por la modalidad de compendio, por lo tanto los resultados clave de esta investigación están contenidos en los artículos principales publicados en revistas que la componen. Además, la información completa acerca de cada artículo puede ser encontrada en el Capítulo 4. Con el objetivo de presentar los principales resultados alcanzados en esta tesis doctoral, cada artículo que la compone es resumido brevemente a continuación.

1.3.1. Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions

El primer trabajo que compone el compendio [119] analiza los principales problemas de seguridad de las tecnologías LPWAN que deben ser abordados y su implicación para la integración de ellas en la arquitectura 5G (**R2**). Este estudio de trabajos analiza la convergencia de escenarios masivos IoT

utilizando mecanismos de seguridad sobre tecnologías de comunicación de bajo consumo dentro del ecosistema 5G (**R1**). El *3rd Generation Partnership Project* (3GPP) pretende incluir IoT como uno de sus esfuerzos de estandarización para la quinta generación de redes celulares. Para conseguirlo, el uso de tecnologías LPWAN es un aspecto clave cuando los dispositivos no tienen acceso a una red eléctrica o connectividad celular disponible. Además, 5G pretende integrar varias redes complejas dentro de su ecosistema. Por este motivo, existe un gran interés en los aspectos de la seguridad de la arquitectura. Sin embargo, esta integración IoT-5G es mermada por los complejos requerimientos de seguridad de la arquitectura 5G, que no permiten ser abordados de forma sencilla por las soluciones LPWAN actuales, dado su severamente limitado canal de comunicación. Primero, se presenta un análisis del estado del arte para la integración de la tecnología NB-IoT, así como otras tecnologías LPWAN no-3GPP dentro de 5G. Adicionalmente, se analiza los requisitos de comunicación encontrados en LPWANs, así como los requisitos de seguridad de casos de uso IoT (**R3**). Después, se presenta un estudio amplio de las propuestas de investigación en el estado del arte para la seguridad dentro del paraguas de las LPWANs. Finalmente, se presentan los esfuerzos desarrollados por las diferentes iniciativas internacionales IoT, así como las organizaciones de definición de estándares. Una contribución destacable de la 3GPP para la integración sin fisuras de redes LPWAN de terceros en el sistema 5G se encuentra en el componente *Non-3GPP Interworking Function* (N3IWF), dedicado para abordar directamente la integración de tecnologías de comunicación radio no-3GPP en 5G. Esto permitiría la integración de tecnologías como LoRaWAN o Sigfox. Este trabajo concluye que las soluciones de seguridad para LPWANs actuales necesitan mejoras y adaptaciones para conseguir la integración sin fisuras con redes 5G. Este hallazgo ha dirigido los subsiguientes esfuerzos de investigación durante la tesis. De este modo, las propuestas presentadas en los siguientes artículos que componen esta tesis se encuentran en la dirección de solucionar las brechas indentificadas en la integración segura de sistemas heterogeneos IoT, entre ellos mismos y con la red 5G.

1.3.2. Impact of SCHC Compression and Fragmentation in LPWAN: A Case Study with LoRaWAN

El segundo trabajo del compendio [120] estudia las diferentes soluciones y requisitos para la transmisión de paquetes basados en IP sobre redes inalámbricas de bajo consumo; específicamente la integración de dispositivos conectados a Internet a través de tecnologías LPWAN (**R1**). La mayoría de las propuestas de investigación previas están inspiradas en los mecanismos de compresión de cabeceras y fragmentación encontrados en las redes basadas en IEEE 802.15.4, como *6LoWPAN* para la transmisión de paquetes IPv6 sobre *low rate wireless personal area networks* (LR-WPANs), RFC4919 [27]. Estos esfuerzos están generalmente divididos en dos categorías. Por un lado, están las tecnologías que utilizan señalización para compartir un contexto entre ambos puntos de la compresión y así realizar la compresión de cabeceras — e.g., Robust Header Compression (RoHC) RFC5795 [28] y el formato de compresión para datagramas IPv6 de redes IEEE 802.14.4 networks (LOWPAN_NHC and LOWPAN_IPHC) RFC6282 [29]. Por el otro lado, están las técnicas *stateless* que prescinden de dicha señalización, ahorrando ancho de banda, pero que generalmente obtienen peor rendimiento — e.g., LOWPAN_HC1 y LOWPAN_HC2 RFC4944 [30]. Tras analizar las desventajas de los mecanismos mencionados, una solución de compresión de cabeceras y fragmentación del estado del arte ha sido implementada (**R4**), Static Context Header Compression (SCHC) RFC8724 [15]. Este mecanismo ha sido estandarizado por el IETF LPWAN work group, teniendo en cuenta todas las características comunes identificadas en la arquitectura LPWAN y sus componentes [9]. Como consecuencia, este trabajo valida la solución mediante la evaluación del rendimiento de SCHC para la transmisión de paquetes IPv6/UDP/CoAP en un banco de pruebas real (**R5**) ejecutándose sobre un despliegue LoRaWAN. Los resultados muestran que la solución permite la transmisión eficiente de intercambios web basados en solicitud y respuesta CoAP, corriendo sobre hardware limitado real sobre LoRaWAN. De este modo, se alcanza la integración completa con Internet y redes IPv6 de hardware embebido sobre tecnologías LPWAN basadas en bandas de radio no licenciadas.

1.3.3. Secure Authentication and Credential Establishment in Narrowband IoT and 5G

El tercer trabajo del compendio [121] analiza los requisitos para protocolos ligeros seguros de acceso a redes celulares sobre LPWAN (**R1**). Este proceso es una parte crítical del *bootstrapping*, el establecimiento seguro de la comunicación en redes 4G/5G (**R2**). Este trabajo propone una arquitectura para autenticación y compartición de claves ligeros sobre NB-IoT, una tecnología LPWAN basada en radio banda licenciada estandarizada por la 3GPP y describe su integración dentro del sistema 5G. Esta propuesta permite el acceso autenticado a redes de terceros fuera de la red celular — conocido como *autenticación secundaria* en 5G. La arquitectura desarrollada ha sido implementada utilizando dos protocolos ligeros para autenticación basados en AAA. Por un lado, el *Protocol for Carrying Authentication for Network Access* (PANA) [31], un protocolo basado en UDP estandarizado por la IETF para permitir la autenticación del acceso a red y establecimiento de claves entre dispositivos y una infraestructura de red. Por el otro lado, *Low-Overhead CoAP-EAP* (LO-CoAP-EAP) [32], una propuesta de investigación se se basa en CoAP, el protocolo de aplicación para intercambios de solicitud y respuesta divisado por la IETF. Gracias al enfoque basado en AAA, este marco ofrece una solución de gestión amigable para humanos, centrada en escenarios escalables masivos de IoT. Adicionalmente, mediante el uso de *Extensible Authentication Protocol* (EAP) [33] y su marco de compartición de claves [34], se obtiene la flexibilidad requerida para soportar dispositivos con recursos computacionales y ancho de banda severamente limitados. El rendimiento de la propuesta ha sido implementado y posteriormente evaluado sobre un banco de pruebas piloto con hardware embebido real corriendo sobre la tecnología NB-IoT, utilizando una banda radio licenciada (**R5**). El rendimiento demuestra que el uso de una solución ligera para autenticación y compartición de claves como LO-CoAP-EAP mejora significativamente el consumo general de batería y el uso de ancho de banda de dispositivos conectados a través de una tecnología LPWAN, convirtiéndose en una solución eficiente y viable para ser utilizada en escenarios masivos IoT sobre 4G/5G.

1.4. Conclusiones y Trabajos Futuros

Gracias al paradigma IoT, servicios y productos nuevos e innovadores están disponibles para resolver problemas complejos encontrados en diferentes verticales. Su presencia tanto en industria y academia está en continuo crecimiento. Las predicciones estiman una continuación de esta tendencia durante los años venideros. Este marco de negocio fomenta diferentes fabricantes a competir, produciendo soluciones que se adaptan a los escenarios de cada cliente. Como consecuencia, se espera que los despliegues masivos IoT tengan un relativamente alto nivel de heterogeneidad. La principal causa es que cada solución de control y monitorización remotos tiene características y propiedades únicas. De entre todas las posibles aplicaciones del paradigma IoT, esta tesis doctoral se centra en soportar Smart Cities, Industry 4.0, Smart Agriculture y similares. Estos son escenarios donde los dispositivos finales están dispersos en una gran área de cobertura. Adicionalmente, no se provee a los sensores de una red eléctrica, ni se espera la disponibilidad de cobertura 4G. Por estos motivos, estos entornos particulares demandan dispositivos que trabajen bajo condiciones climáticas adversas, sin supervisión humana, compartiendo el canal de comunicación con hasta cientos o miles de dispositivos diferentes.

Las industrias verticales mencionadas se benefician de varios indicadores clave de rendimiento, principalmente: reducir el coste por dispositivo, incrementar el radio de cobertura y mejorar la autonomía de la batería del dispositivo. Estas aplicaciones han recurrido a dispositivos basados en chips microcontroladores de bajo consumo, ejecutando aplicaciones con una programación ligera, volcando tanta complejidad como sea posible al lado no limitado de la infraestructura — e.g., plataformas y servicios en la nube. Mediante la combinación de estos tres indicadores clave de rendimiento, la solución más prometedora para estos escenarios son las redes LPWAN. Estas se centran en proveer con una solución de conectividad barata a áreas geográficas extensas, permitiendo largos ciclos de vida de baterías y reduciendo el coste por unidad. La elección de tecnología LPWAN tiene una gran relevancia

en el rendimiento general del despliegue, así como los escenarios soportados, puesto que los dispositivos finales consumen la mayor cantidad de su energía transmitiendo información.

Cuando esta oportunidad de negocio apareció, diferentes fabricantes se dieron cuenta de que lanzar soluciones al mercado rápidamente era esencial. Por lo tanto, diferentes empresas y organizaciones se apresuraron en lanzar productos y servicios tan rápido como fuera posible, con la esperanza de capitalizar el mercado antes que la competencia. Desafortunadamente, esta carrera impetuosa llevó a decisiones de diseño apresuradas, hechas durante el camino a obtener la solución. Algunas de estas decisiones todavía plagan despliegues actuales con impedimentos pendientes de resolver. Esto es una consecuencia de los enfoques radicalmente diferentes que cada fabricante decidió adoptar para su solución LPWAN, en términos tanto técnicos como de modelo de negocio. Por ejemplo, Sigfox se dispuso a proveer una plataforma todo-en-uno cerrada y privada, liberando así a los clientes de las características técnicas de su servicio, exigiendo únicamente de sus clientes una cuota mensual por cada uno de los dispositivos utilizados.

Contrariamente, LoRaWAN optó por un enfoque más abierto, haciendo la especificación de la capa MAC disponible públicamente, así como otros documentos técnicos. Además, esto permitió un modelo de negocio basado en servicios en torno a redes LoRaWAN, donde cualquiera puede implementar y desplegar libremente componentes de la arquitectura y cobrar a otros por sus servicios. Los clientes son libres de elegir entre implementar su propia versión de la red o contratar los servicios de cualquier proveedor de su elección. Para responder de forma rápida al surgimiento de varias opciones en el mercado, la respuesta de la 3GPP fue estandarizar rápidamente tanto NB-IoT como LTE-M, dos tecnologías diferentes con una propiedad clave en común: ser desplegables por cualquier teleoperador con una actualización de software sobre su core 4G/LTE y estaciones base. Así, se otorgaría a NB-IoT y LTE-M de una gran ventaja, puesto que hay una gran cantidad de infraestructura celular ya desplegada globalmente. Sin embargo, los clientes finales dependen de que su teleoperador local decida aplicar esta actualización de software y proveer de estos servicios antes de poder utilizarlos, además del coste mensual que conllevaría la contratación de dicho servicio.

Por todos estos motivos, la integración de las tecnologías LPWAN dentro del paradigma IoT es un tema de gran interés tanto para academia como industria. Esto no es únicamente un problema de ingeniería de comunicaciones, si no que tiene varios matices relacionados con el tipo de data que está siendo transmitido y sus implicaciones. Por este motivo, la confidencialidad y privacidad de los datos es otro reto asociado a las LPWANs para alcanzar la integración sin fisuras con otros despliegues. Varias SDOs tratan de conseguir mecanismos de seguridad y confianza alcanzables sobre entornos limitados, dado que cada LPWAN utiliza soluciones de seguridad a medida que no son interoperables con otros despliegues. Todo esto ha propiciado la aparición de islas de conectividad aisladas unas de otras, donde dispositivos pertenecientes a un dominio administrativo o tecnología, son incapaces de comunicarse con otros. Esto contradice la estrategia de integración abierta y sin fisuras que promueve el paradigma IoT.

Para abordar todos los problemas de la integración IoT-LPWAN, la meta principal del periodo de trabajo de esta tesis doctoral ha sido desarrollar, implementar y evaluar protocolos seguros para el paradigma IoT sobre tecnologías de largo alcance y bajo consumo. Primero, el ecosistema celular 5G fue identificado como un elemento clave en el éxito de los escenarios IoT masivos para monitorización y control remotos. Por este motivo, fue añadido como un objeto de estudio en las etapas tempranas de esta tesis. Así, los requisitos de comunicación de las verticales IoT fueron estudiados bajo el paraguas de los entornos limitados, específicamente aquellos alimentados por batería utilizando LPWANs. Diferentes propuestas de investigación fueron sondeadas para proveer de un acceso seguro y autenticado a puntos fuera de la infraestructura LPWAN/celular, a través de procedimientos *bootstrapping* ligeros [119].

Para permitir la integración sin fisuras de dispositivos IoT, los esfuerzos de estandarización de la IETF promueven el uso del protocolo de red IPv6, debido al declive en el espacio de direcciones de IPv4. Normalmente, la adopción de IPv6 como una base fundamental de comunicaciones sobre Internet no supondría un problema en otros entornos computacionales. Sin embargo, debido a las severas limitaciones del ancho de banda sufridas por LPWANs, transmitir la relativamente grande cabecera obligatoria de 40 bytes es prohibitivamente caro, en términos de recursos radio consumidos. Para alcanzar la interoperación de diferentes dispositivos conectados a través de redes LPWAN con

Internet, el mecanismo *Static Context Header Compression* (SCHC) propuesto por la IETF LPWAN WG ha sido implementado y validado [120]. La evaluación sugiere que SCHC es una solución eficiente para la transmisión de paquetes basados en IP sobre LPWANs.

Las soluciones LPWAN son diversas en lo que se refiere a su capa MAC, la cuál es diseñada considerando la tecnología radio utilizada en la capa física. Por este motivo, los fabricantes ofrecen mecanismos de seguridad relativamente sencillos que dependen de alguna variante de criptográfica simétrica, cuya clave es instalada durante la programación en ambos, dispositivo final y plataforma que lo soporta. Esto ha motivado la consecución de soluciones interoperable y de estandarización abierta, que pueden ser ejecutados sobre entornos limitados. Para abordar esto, un mecanismo ligero de autenticación y compartición de claves para redes de largo alcance y bajo consumo fue implementado sobre una red NB-IoT real. Tras la evaluación, la investigación concluye en que el uso de LO-CoAP-EAP es una solución *bootstrapping* válida para proveer de un marco escalable y amigable para humanos de autenticación basado en AAA en LPWANs [121].

Finalmente, los esfuerzos de ambos trabajos [120] y [121] han sido combinados para diseñar y proponer un procedimiento *bootstrapping* eficiente, seguro y ligero para la autenticación y compartición de claves, basado en LO-CoAP-EAP, el cuál ha sido implementado y evaluado sobre una red LoRaWAN real en un escenario móvil de Smart City. Esta contribución también permitió la integración sin fisuras de dispositivos IoT a través del mecanismo SCHC para la compresión y fragmentación de paquetes IPv6. Como resultado, el trabajo [127] muestra cómo la solución propuesta provee a dispositivos LoRaWAN de la capacidad para interoperar de forma segura con cualquier dominio tercero conectado a través de Internet, gracias a IPv6, mientras que se promueve un sistema de gestión amigable para humanos y escalable para la autenticación y autorización de escenarios masivos IoT.

Las vías futuras propuestas para este trabajo están orientadas hacia soportar un mayor conjunto de dispositivos, incluso con limitaciones de conectividad y comunicación más severas. Nos gustaría puntualizar que durante esta tesis doctoral, fuimos contactados por el departamento de comunicaciones satelitales de la Agencia Espacial Europea (*European Space Agency*, ESA). Han expresado su interés en nuestra solución propuesta y validada en [120], [127]. Esperamos en el futuro próximo integrarla en el paraguas de comunicaciones LoRaWAN satélite y realizar pruebas experimentales. Después, es nuestra intención alinear nuestra investigación con los esfuerzos de estandarización de los *work groups* IETF ACE y LPWAN, sobre problemas de conectividad y seguridad para dispositivos limitados. Particularmente, nos gustaría investigar la compresión de protocolos seguros, principalmente *Object Security for Constrained RESTful Environments* (OSCORE) y *Ephemeral Diffie-Hellman Over COSE* (EDHOC).

Siguiendo con esta línea de investigación, el rendimiento general de las redes LPWAN se beneficiaría en más de un modo. Por ejemplo, un trabajo de estandarización que está ganando inercia es el *Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework* (ACE-OAuth) [35]. Un protocolo de estandarización que puede apoyarse en EDHOC y OSCORE. Finalmente, otro de los temas de interés que abarca todas las áreas relacionadas con IoT es el uso de modelos generados mediante *Machine Learning* (ML) que pueden ser ejecutados sobre hardware embebido, para mejorar a través de datos estadísticos el rendimiento general y la seguridad de LPWANs.

CHAPTER 2

Abstract

2.1. Motivation

The Internet of Things (IoT) is a term first coined in 1999 [1] referring to the intercommunication of RFID chips over the Internet. However, in the present day, IoT encompasses a higher concept. The IoT introduces a paradigm that expands the reach of the Internet beyond digital resources, by enabling remote access and control of physical resources through IP-based communication protocols [2]. Historically, significant advancements in computer networks have always been oriented towards human-centered communications, where humans are both, the main producers and consumers of the information circulating the Internet. For this reason, achieving a better human-centric Internet experience through better bandwidth and lower latency for accessing digital resources was one of the main goals of both industry and academia. However, the IoT considers that machines produce and consume a growing amount of data when compared to human-centric exchanges.

The IoT has heavily impacted both society and industry-related activities. Earlier, the different commercial services and products included the IoT paradigm as an afterthought when the target was already finished. But, in recent years, the IoT paradigm is now part of the design stage itself, considered even before the business plan is drafted. The revenue volume from IoT-related activities is continuously growing [3], [4]. It is estimated that 18 billion devices will be connected to the Internet by 2022 [5]. Also, since the definition of what actually is an IoT device varies for different institutions, the estimation values may change in different reports. Fig. 2.1 shows the growth of connected IoT devices by another report, which states that there will be over 25 billion connected IoT devices by 2030 [6]. Additionally, it is expected that the global IoT market will reach USD1.567 trillion by 2025 [7]. As a consequence, IoT has become a topic of interest for both industry and academia, affecting most of the productive fabrics in diverse scenarios. In essence, IoT creates value by connecting devices measuring and actuating over their physical environment, in a cooperative way. This enables, not only remote control and monitoring, but also gathering valuable statistical data, that can be analyzed to obtain knowledge and solve complex problems in an unprecedented way. Some application examples include use cases for Smart Cities, Smart Buildings, Industry 4.0, Smart Agriculture, e-Health, and Intelligent Transportation Systems.

Previous to IoT widespread, different verticals already employed information technologies for remote monitoring and control. These leverage on embedded hardware that is connected to several electro-mechanical sensors and actuators, reporting data back to a centralized component. The deployment administrators have human-readable access to the current state of the whole system through what is

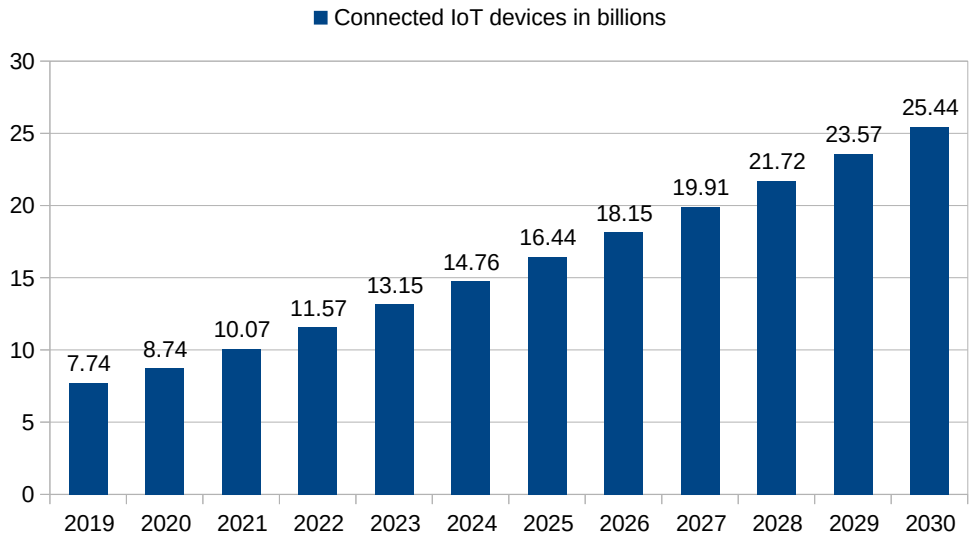

Figure 2.1: Connected IoT devices in billions prevision. Source [6]

called Supervisory Control And Data Acquisition (SCADA). The last-mile infrastructure that supports the remote control and monitoring tasks is known as Wireless Sensor Networks (WSNs). These predate the IoT paradigm and have been implemented with a myriad of vendor-specific technologies that implement ad-hoc solutions for communication and security problems, designed around the end-device and radio technology constraints. What sets the IoT apart from the WSNs is a prominently higher level of compatibility. This is achieved through employing Internet-based protocols at the network layer. Hence, deployments belonging to different administrative domains, or leveraging on vendor-specific platforms, are expected to interoperate through IP-based networks.

Thanks to its benefits, the IoT industry drives the apparition of market-ready products and services in different application areas. For this reason, devices compose a diverse and heterogeneous environment, performing a wide range of functionalities. These range from the inclusion of a very specific operation logic, like a remotely controlled lightbulb, to a more generic device, like an smartphone. Additionally, IoT devices have a wide range of computational characteristics, ranging from embedded microcontroller-devices, up to applications running in commodity hardware. Also, the nature of the communication bandwidth varies widely, ranging from devices that stay most of the time in an inactive state and send short messages periodically, to devices that perform critical tasks and require ultra-low latency communication channels to a high-volume broadband link. As a consequence, one of the major challenges associated with IoT scenarios is procuring engineering solutions that employ a set of protocols or technologies tailored to the devices' characteristics and the employed network.

There is a subset of applications that has greatly benefited from remote control and actuation technologies. These scenarios include Smart Cities, Industry 4.0, and Smart Agriculture, among others. They are enabled by sensor and actuator embedded devices scattered in a large geographical area, typically working without human supervision, lacking access to power-grids, and outside the reach of cellular networks. The specific requirements found in these scenarios present a large set of challenges and gaps for current IoT communication technologies. A novel paradigm has partially filled this communication gap is Low-Power Wide-Area Networks (LPWANs) [8]–[14]. They reduce the cost-per-device by employing low-power long-range radio technologies that can cover a vast area with fewer base-stations, which support a larger number of devices per cell. However, LPWANs are limited to highly constrained communication channels, designed to support sporadic short transmissions at relatively low data-rates — in the order of bps or kbps. Consequently, another major gap found in LPWAN-based scenarios is security and privacy, due to their preference for vendor-specific simpler network stacks, aimed at reducing the total header overhead. For this reason, the common technologies

employed for Internet security and privacy are not feasible in constrained networks, due to their prohibitively large header size and number of required transmissions. Thus, LPWANs spawn vendor-specific isolated islands of communication, preventing the secure and private interoperation of embedded devices through the Internet. This contradicts the very essence of the IoT paradigm, which leverages in the use of openly standardized Internet protocols to foster a cohesive and interoperable environment, where different entities collaborate sharing information about their environment, solving difficult problems.

The present PhD thesis describes the research results of the design, implementation, and validation of novel secure protocols for the Internet of Things leveraging on low-power communication technologies. These protocols enable the secure communication of embedded devices with the Internet over LPWAN technologies, adapting to each use case scenario and deployment characteristics. The interoperable communication of end-devices over the Internet is provided through IPv6 thanks to the Static Context Header Compression (SCHC) RFC8724 [15]. This mechanism supports the interoperable communication of devices belonging to different administrative domains and employing different LPWAN flavors. This enables an heterogeneous variety of battery-powered devices to be deployed over technologies such as Sigfox [16], LoRaWAN [17], Narrowband-IoT (NB-IoT) [18]–[22], or Long Term Evolution for Machines (LTE-M) [10]. To provide security and privacy to the communications, as well as an scalable and human-centric management solution for massive heterogeneous deployments, the devices perform a lightweight authenticated key agreement scheme based on an standardized Authentication, Authorization, and Accounting (AAA) framework [23], [24]. After evaluation of different application layers, these contributions are aligned to the use of Constrained Application Protocol (CoAP) [25], considered by the Internet Engineering Task Force (IETF) as one of the key building blocks in future constrained environments, enabling a web-based request-answer resource access in delay tolerant and lossy scenarios [26].

This PhD was supported by the Seneca Foundation[1] in Murcia Region (Spain) through the FPI Program (Grant No. 20751/FPI/18) and partially funded by Odin Solutions S.L.[2]

2.2. Goals and Methodology

The aforementioned set of challenges and gaps in current IoT communications for low-powered environments have driven the developments and contributions contained in this thesis. It is intended to establish a foundation for low-power sensor and actuator networks that require interoperable and secure access to third-party deployments through Internet-based protocols. The methodology was achieved by combining network engineering problems regarding the efficient transmission of IP-based packets over low-power networks. In a second part, the methodology focuses on the design and implementation problems that arise from establishing secure and private interoperable deployments over low-power networks, following the IoT paradigm key principle of using the Internet as a common ground. Then, both parts were merged to achieve the efficient interoperation of constrained end-devices over low-power networks through the Internet in a secure and private way. Thorough the development of this thesis, its different contributions where integrated in the results of European H2020 projects Fed4IoT[3], CYSEMA[4], and European H2020 open call project IoTrust[5]. Finally, the research proposal was validated using LPWAN technologies over both unlicensed and licensed radio bands deployments. Thus, the research objectives of this thesis are as follows:

- Objective 1: Study the feasibility and requirements for embedded devices securely transmitting IP-based protocol packets over LPWANs.

[1] http://fseneca.es/
[2] https://www.odins.es/en
[3] https://fed4iot.org/
[4] https://www.iot4industry.eu/project_cysema
[5] https://www.odins.es/en/iot-trust-security-on-internet-of-things/

- Objective 2: Analyze the state-of-the-art solutions to securely integrate third-party vendor LPWANs within 4G and 5G cellular systems.
- Objective 3: Study and analyze header compression and fragmentation mechanisms for the transmission of IP-based packets over low-power communication technologies.
- Objective 4: Study and analyze lightweight secure authentication and key agreement techniques for constrained environments.
- Objective 5: Implement an efficient header compression and fragmentation mechanism for the transmission of IP-based packets over low-power communication technologies.
- Objective 6: Implement an scalable and human-centric lightweight secure authentication and key agreement technique for constrained environments.
- Objective 7: Integrate and validate on real-life hardware an efficient compression and fragmentation mechanism for the transmission of IP-based packets over low-power communication technologies.
- Objective 8: Integrate and validate on real-life hardware the secure and authenticated communication of embedded devices over LPWAN.

The process followed to pursue these objectives consisted in establishing sublines of research associated to each of the objectives, which finally converge as a whole to compose this thesis. All of these objectives were repeatedly addressed, following an iterative incremental methodology. Each pass output generates new knowledge in a closed feedback loop that improves and refines the next iterations. The different phases include requirement analysis, state-of-the-art research, proposal design, evaluation, and validation. Following this methodology improves the results achieved by each objective and shape the overall contribution.

In this regard, to study the computational and communication requirements of constrained environments, a real-life scenario was deployed with embedded and radio infrastructure hardware to achieve LPWAN scenarios using both unlicensed and licensed radio band-based technologies, consisting in LoRaWAN and NB-IoT, respectively. Next, an analysis of state-of-the-art alternatives was performed for integration of third-party low-power IoT technologies in cellular networks, particularly 5G systems. Then, the requirements of transmitting IPv6/UDP packets over LPWANs were studied. As a consequence, several header compression and fragmentation alternatives were analyzed. This led to the design, implementation, and validation of a IPv6/UDP/CoAP header compression mechanism based in IETF standardization efforts, for the integration of constrained devices within the Internet — SCHC. Finally, the integration of different Internet-based security and privacy mechanisms within the constrained ecosystem was analyzed. This led to the design, implementation, and validation of a lightweight authenticated key agreement mechanisms based on AAA infrastructures using an IP protocol stack over lossy and delay-tolerant networks.

2.3. Results

The contributions of the aforementioned objectives of this PhD thesis derived in several scientific publications in impact journals and international conferences, as presented at the end of Chapter 5. The key results are shown in Table 2.1, displayed together with their addressed objectives. Furthermore, the work developed during the thesis has been employed in several european funded research projects, as described in Section 2.2. Additionally, it has extended the discussion of standardization efforts by the IETF to integrate embedded devices within the Internet ecosystem, especially for IETF's LPWAN and ACE work groups. Note that this thesis has been presented by the compendium modality, thus the key results of this research are found contained inside the main journal publications that comprise it. Also, the full information about each article can be found in Chapter 4. In order to present the main research results achieved in this PhD thesis, each composing article is is briefly summarized below.

Table 2.1: Main thesis results

Result	Objectives	Publications
R1. Analysis of the requirements for embedded devices securely transmitting IP-based protocol packets and analysis of the deficiencies in the current solutions for the integration of LPWAN technologies in the IoT paradigm.	1,2	[119] [120] [121] [122] [123]
R2. Analysis of the state-of-the-art solutions to securely integrate third-party vendor LPWANs within cellular systems.	1,2,3	[119] [121] [123] [124]
R3. Implement a lightweight secure authentication and key agreement technique for constrained environments through suitable techniques and tools for this paradigm, to address scalability and human-centric management of heterogeneous IoT deployments.	4,6	[119] [121] [124] [125] [126] [127]
R4. Implement an IPv6/UDP/CoAP header compression and packet fragmentation mechanism based in IETF standardization efforts in order to integrate constrained environments with the Internet.	3,5	[120] [125] [126] [127]
R5. Validation and evaluation of the proposed solutions in a real-life scenario in order to verify their feasibility.	5,6,7,8	[120] [121] [127]

2.3.1. Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions

The first work of the compendium [119] analyzes the main security issues of LPWAN technologies that must be addressed, and their implications for integrating them within the 5G architecture (**R2**). This survey of works analyzes the convergence of massive IoT scenarios using security mechanisms over low-power communication technologies within the 5G ecosystem (**R1**). The 3rd Generation Partnership Project (3GPP) aims at including IoT as one of its main standardization efforts for the fifth generation of cellular networks. To do so, the use of LPWAN technologies is a key aspect when end-devices do not have access to power-grids or broadband access points deployments nearby. Also, 5G aims to integrate a lot of complex networks within its ecosystem. For this reason, a lot of effort is put into the security aspects of the architecture. Nevertheless, this IoT-5G integration is hindered by the complex security requirements of the 5G architecture, which are not always addressable in a simple manner by LPWAN solutions, given their severely constrained communication channel. First, it presents an analysis of the state-of-the-art for integrating the NB-IoT technology, as well as other non-3GPP LPWANs within 5G. Additionally, it analyzes the security communication requirements found in LPWANs, as well as the IoT use-case security requirements (**R3**). Next it presents a broad survey of the state-of-the-art security research contributions found under the umbrella of LPWANs. Finally, it presents the efforts developed by several IoT international initiatives as well as standard developing organizations. One noteworthy contribution of the 3GPP to the seamless integration of third-party LPWANs within the 5G ecosystem is the Non-3GPP Interworking Function (N3IWF), an architecture component devised to directly addresses the integration of non-3GPP radio access technologies within 5G. This would allow the integration of technologies such as LoRaWAN or Sigfox. This work concludes that current LPWAN security solutions need further enhancements and adaptations in order to achieve seamless integration with 5G networks. This finding has directed subsequent research efforts during the thesis. This way, the presented proposals in the following articles that compose this thesis are aimed at addressing the identified gaps to achieve the secure integration of heterogeneous IoT systems, among themselves and with the 5G network.

2.3.2. Impact of SCHC Compression and Fragmentation in LPWAN: A Case Study with LoRaWAN

The second work of the compendium [120] studied the different solutions and requirements for the transmission of IP-based packets over low-power radio networks; specifically, the integration of devices connecting to the Internet through LPWAN technologies (**R1**). Most state-of-the-art research proposals are inspired in the use of header compression and fragmentation mechanisms employed for IEEE 802.15.4 networks, such as *6LoWPAN* for the transmission of IPv6 packets over low rate wireless personal area networks (LR-WPANs), RFC4919 [27]. These efforts are broadly split in two separate categories. On the one hand, there are the technologies that use signaling to share a context among both compression end-points to perform the header compression — e.g., Robust Header Compression (RoHC) RFC5795 [28], and the compression format for IPv6 datagrams over IEEE 802.15.4 networks (LOWPAN_NHC and LOWPAN_IPHC) RFC6282 [29]. On the other hand, there are stateless solutions that do not perform such signalling, saving radio bandwidth, but are generally speaking less efficient — e.g., LOWPAN_HC1 and LOWPAN_HC2 RFC4944 [30]. After analyzing the drawbacks of the aforementioned mechanisms, a state-of-the-art header compression and fragmentation mechanism was implemented (**R4**) — Static Context Header Compression (SCHC) RFC8724 [15]. This mechanism has been standardized by the IETF's LPWAN work group, taking into consideration all the common traits identified in LPWANs architecture and components [9]. As a consequence, this work validates the solution by evaluating the performance of SCHC for the transmission of IPv6/UDP/CoAP packets in a real-life test-bed (**R5**) running over a LoRaWAN deployment. The results showed that the solution allows the efficient transmission of CoAP web-based request-answer exchanges running on real-life constrained hardware through LoRaWAN. Therefore, the complete integration with the Internet and IPv6 networks is achieved for embedded hardware over unlicensed radio band LPWAN technologies.

2.3.3. Secure Authentication and Credential Establishment in Narrowband IoT and 5G

The third work of the compendium [121] analyzes the requirements for lightweight and secure protocols to access to cellular networks over LPWANs (**R1**). This process is a critical part of the bootstrapping process, the secure establishment of communications in 4G/5G networks (**R2**). The work proposes an architecture for lightweight authentication and key establishment over NB-IoT, a licensed radio band LPWAN technology standardized by the 3GPP, and describes its integration within the 5G system. This proposal enables authenticated access to third-party networks outside of the cellular network — known as *secondary authentication* in 5G. The presented architecture was implemented using two different AAA-based lightweight authentication mechanisms. On the one hand, the Protocol for Carrying Authentication for Network Access (PANA) [31], an UDP-based protocol standardized by the IETF to enable authentication for network access and key establishment between devices and a network infrastructure. On the second hand, Low-Overhead CoAP-EAP (LO-CoAP-EAP) [32], a research proposal that builds on top of CoAP, the web-based request-answer application layer envisioned by the IETF. Thanks to the AAA-based approach, this framework offers a human-centric management solution for scalable and heterogeneous massive IoT scenarios. Additionally, the use of the Extensible Authentication Protocol (EAP) [33] and its key management framework [34], facilitates the flexibility required by supporting devices with severely constrained computational and bandwidth resources. The performance of the proposal has been implemented, and later evaluated over a pilot test-bed with real-life embedded hardware running over a NB-IoT LPWAN technology, employing a licensed radio band (**R5**). The performance demonstrates that the use of a lightweight authentication and key agreement solution like LO-CoAP-EAP significantly improves the overall battery-life and bandwidth usage of devices connected to LPWAN technologies, becoming a feasible and efficient solution to be used in 4G/5G massive IoT scenarios.

2.4. Conclusions and Future Work

Thanks to the IoT paradigm, novel and innovative services and products are available to solve complex problems found in all different verticals. Its presence in both industry and academia is steadily growing. Foreseeable predictions estimate the continuation of this trend for years to come [6]. This business framework drives several vendors to compete, producing solutions that adapt to each customer's scenario. As a consequence, massive IoT deployments are expected to have a relatively high level of heterogeneity. The main cause is that each remote monitoring and control solution has unique quirks and characteristics. Out of all the possible applications for the IoT paradigm, this PhD thesis focuses in supporting Smart Cities, Industry 4.0, Smart Agriculture, and the like. These are scenarios where end-devices are dispersed in a large coverage area. In addition, they do not provide sensors with a power-grid, or expect the availability of 4G coverage signal. For the aforementioned reasons, these particular environments call for devices working under harsh climate conditions, without human supervision, sharing the communication channel with up to hundreds or even thousands of different devices.

The aforementioned verticals benefit from different key performance indicators, namely, reducing the per-device cost, increasing the radio coverage range, and improving the battery-life autonomy. These applications resorted to devices based on low-power microcontroller chips, running simple applications in a lightweight firmware, dumping as much complexity as possible in the supporting side of the infrastructure — e.g., cloud platforms, back-haul network. By combining all three key performance indicators, the most promising solution for these scenarios are LPWANs. These focus on providing inexpensive connectivity to expanse geographical areas, enabling long battery life-cycles, and reducing the per-device unit price. The election of an LPWAN technology has a great relevance on the overall deployment performance and supported scenarios, since end-devices spend the majority of their energy transmitting data.

When this business opportunity appeared, different vendors realized that time to market was of the essence. Hence, many different companies and organizations hurried to launch products and services as quickly as possible, in hopes of capitalize the market before the competence. Regrettably, this impetuous race led to hastily decisions made on the way to producing a solution. Some of these still plague current deployments with hindrances that are yet to be solved. This is a consequence of the radically different approaches that each vendor decided to follow for their particular LPWAN solution, in terms of both technical characteristics and business model. For instance, Sigfox aimed to provide an closed and private all-in-one solution that freed customers from the technical characteristics of their marked solutions, only requesting customers to pay a monthly fee per device in return.

Conversely, LoRaWAN opted for a more open approach, making publicly available the MAC layer specification and other technical documents freely. Also, this allowed a service-based business model revolving around LoRaWAN networks, where anyone is free to implement, deploy, and charge others for the use of their infrastructure. End-customers are free to choose between implementing the required components themselves, or hire the services of any vendor of their choosing. To provide a timely answer to the spawning options in the current market, the 3GPP answer was to quickly standardize both NB-IoT and LTE-M, two different LPWAN technologies with one key thing in common, namely, both can be deployed by any telco service provider with a software update to their 4G/LTE core and base-stations. Hence, giving NB-IoT and LTE-M a considerable head-start, due to the extensive cellular infrastructure already globally present. However, end-customers are dependable of their local service provider telcos to deploy such technologies in their assets, besides the monthly fees that would result from hiring the service.

For all the aforementioned issues, the integration of LPWAN technologies within the IoT paradigm has become of great interest for both academia and industry. This is not only a pure communication engineering problem, but it has several nuances related to what kind of data is being transmitted over radio and its implications. For this reason, data confidentiality and privacy is another challenge associated with LPWANs for achieving seamless interoperation with other deployments. Several SDOs aim at enabling security and trust mechanisms that are achievable over constrained environments,

since each LPWAN vendor employs tailored security solutions that are not interoperable with other deployments. This is further exacerbated since some vendors decide to not publish security-related information about their solutions. All of this, generates connectivity isolated islands, where devices belonging to a specific administrative domain or technology, are unable to communicate with other parties. This contradicts the seamless and open interoperation strategy that the IoT paradigm promotes.

To address all the IoT-LPWAN integration issues, the main goal of this PhD thesis research period has been to design, implement, and evaluate novel secure protocols for the IoT paradigm over long-rang low-power technologies. At first, the 5G cellular ecosystem was identified as a major player in the success of massive IoT scenarios for remote monitoring and control applications. For this reason, it was included as a study subject for the early stage of this research thesis. Thus, the communication requirements of IoT verticals were studied under the umbrella of constrained environments, specifically battery-powered constrained devices using LPWAN solutions. Different research proposals were surveyed in order to provide a secure and authenticated access to end-points outside of the supporting LPWAN/cellular infrastructure, through lightweight bootstrapping procedures [119].

To enable the seamless integration of IoT devices, the IETF standardization efforts promote the use of the IPv6 network protocol, due to the current decline of IPv4 address space. Normally, the adoption of IPv6 as a building block for Internet-based communications would not be an issue in other computation environments. However, due to the stringent communication bandwidth limitations suffered in LPWANs, transmitting the relatively large 40-byte mandatory header is prohibitively wasteful, in terms of employed radio channel resources. To achieve the interoperation of different LPWAN connected devices with the Internet, the Static Context Header Compression (SCHC) mechanism proposed by the IETF LPWAN WG has been implemented and validated [120]. The evaluation suggests that SCHC is an efficient solution for the transmission of IP-based packets over LPWANs.

LPWAN solutions are diverse with regards to their MAC layer, which in turn has been designed with the radio technology employed in the physical layer. For this reason, vendors provide relatively basic security mechanisms that rely in some form of symmetric key encryption, which is installed at the programming time in both, the device and the supporting platform. This has motivated seeking interoperable and openly standardized solutions that can be run over constrained environments. To address this, a lightweight authentication and key agreement mechanism for long-range low-power networks was implemented and validated over a real-life NB-IoT network. After evaluation, the research concludes that use of LO-CoAP-EAP bootstrapping is valid solution to provide an scalable and human-centric AAA-based authentication framework for LPWANs [121].

Lastly, the efforts of both works [120] and [121] have been combined to design and propose an efficient lightweight secure authentication and key agreement bootstrapping procedure, based in LO-CoAP-EAP, which was implemented and evaluated over a real-life LoRaWAN mobile Smart City scenario. This contribution also enabled the seamless integration of IoT devices through the SCHC mechanism for IPv6 packet compression and fragmentation. As a result, the work [127] illustrates how the proposed solution enables LoRaWAN devices the capacity to interoperate securely with any third-party domain connected to the Internet, while enforcing an scalable human-centric management system for the authentication and authorization of massive IoT scenarios.

Future ways proposed for this work are directed at supporting even a larger set of devices, with even more constrained connectivity and computational limitations. We would like to point out that during this PhD research period, we were contacted by the Satellite Communications Department at the European Space Agency (ESA). They expressed their interest in our solution proposed and validated in [120], [127]. We expect in the near future to integrate it within the umbrella of satellite LoRaWAN communications and perform experimental tests. Next, it is our intention to align our research with the state-of-the-art standardization efforts by both IETF ACE and LPWAN work groups, with regards to connectivity issues and security for constrained devices. Particularly, we would like to research the compression of security related protocols, mainly Object Security for Constrained RESTful Environments (OSCORE) and Ephemeral Diffie-Hellman Over COSE (EDHOC).

By following this line of research, the overall performance of LPWAN networks would benefit in more

than one way. For instance, one standardization effort that is gaining traction is the Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth) [35]. An standardization effort that may leverage on both EDHOC and OSCORE. Lastly, another interesting topic of research that permeates all areas related to IoT is the use of Machine Learning (ML) generated models that can be run in the embedded hardware, for improving through statistical data the overall performance and security of LPWANs.

CHAPTER 3

Introduction

The first appearance of the Internet of Things (IoT) as a concept can be traced back to the year 1999 [1], originally referring to linking the RFID-based supply chain to the Internet. However, the author did not expect that years later the term would become one of the most relevant topics of social, economic, and technical relevance.

The IoT is a technical paradigm that has affected most, if not all, the productive fabrics in diverse applications and contexts. It can be defined as the extension of the Internet connectivity to the physical realm. Previously, the Internet was envisioned as a medium to access digital resources, e.g., images or documents. In that case, the geographical location of the entities actually serving the resource is irrelevant, and not provide any value to the requester. By contrast, the IoT pretends to extend such reach to physical resources, like the current temperature of a remote room or the speed of a specific vehicle. This communication is bi-directional, and as such, it allows the actuation over physical resources, such as closing irrigation valve located in a farming crop. In order to achieve such paradigm, end-devices must equip sensors and actuators, as well as be remotely accessible through some form of communication technology [36].

The IoT can be employed in several different disciplines leveraging on the convergence of different interdisciplinary technologies [2]. In recent years, market-ready solutions for devices that enable sensorization and actuation have proliferated. Several of these solutions have become increasingly more affordable and have sprouted novel applications such as Smart Cities, Smart-Buildings, Smart Agriculture, Industry 4.0, and Smart Grids. Likewise, the results attained from IoT have driven even more advancements in these sensorization solutions, creating a virtuous-cycle, where these verticals are enabled by the technology advancements, and the technology improves driven by the demand in several interdisciplinary scenarios.

Since the dawn of this paradigm, the revenue volume from the IoT-related industries is in continuous growth [3], [4]. At the same time, this tendency has driven a continuous increase in the number of devices connected to the Internet. It is expected that there will be 18 billion connected devices by 2022 [5]. The IoT paradigm fosters innovative and novel business models where creativity and out-of-the-box thinking can result in extremely valuable products and services. In principle, IoT considers on the creation of value through the thoughtful consideration of physical entities collaborating in the resolution of complex problems by sharing data. Some typical examples include individuals, vehicles, production lines, farming crops, and buildings as connected entities.

The IoT was not the original paradigm centered around sensors and actuators for such scenarios. Much earlier, Wireless Sensor Networks (WSN) predated the IoT in terms of remote monitoring and

actuation. WSNs overlap with IoT in the sense that both leverage on end-devices reporting data about their environment. Typically, WSN-based remote monitoring and actuation platforms have a star topology with a central component running a Supervisory Control And Data Acquisition (SCADA). It implements the higher level logic to solve complex problems. The main function of SCADAs is to serve a human-friendly control dashboard of the overall status of the system, in order to allow operators to make complex business decisions, and to gather data that can be analyzed later on for reports.

There is a set of specific verticals that have greatly benefited from the remote monitoring and actuation paradigm. These are scenarios leveraging on sensor devices deployed in geographically sparse areas, installed in hard-to-reach locations, and intended to work autonomously, without regular human supervision. Typically, this approach can be found in several scenarios, mainly related with Smart Cities, Industry 4.0, and Smart Agriculture, as mentioned previously.

Compared to WSNs, IoT presents a different approach. On the one hand, WSNs typically employ ad-hoc networking solutions heavily tailored to the specific use case and deployment in place. In these cases, industrial vendor-specific solutions are mostly employed, which are typically not interoperable with other solutions or deployments, even those marketed by the same vendor. On the other hand, IoT prioritizes the integration of heterogeneous devices and networks through open specification Internet-based protocols, such as those relying in protocols like IP, TCP, or UDP. One of the major advantages of IoT is its capacity to integrate legacy systems, acting as a bridge or adapter in a way that pre-established deployments or solutions can benefit from this paradigm, enabling interaction with other elements connected to the Internet. Precisely for this reason, the IoT has gained even more attention as a paradigm, due to the continuous trend to integrate legacy WSNs with Internet-based technologies and existing individual solutions with vendor-specific dependencies, moving towards a novel, distributed, and interoperable service ecosystem.

The IoT paradigm sets itself further apart from legacy sensor networks by enabling high level interoperability. This is, IoT applications do not require a centralized and vendor-specific platform, instead, leveraging on open standardized IP-based protocols enable deployments from different administrative domains to interoperate — e.g., different telco operator deployments. This drives the creation of novel, highly dynamic, and extensible business models and market opportunities. The IoT is a paradigm that allows specialized modular services to be provided to different clients and within different commercial products. For instance, a data monitoring sensor network deployment can be rented to third parties in the form of Sensors-as-a-Service. Recently, these strategies have become highly desirable in contrast with previously established services and products. There is a new trend in the way innovative technological projects are approached based on the observation that, broadly speaking, Moore's Law is not applicable anymore [37], [38]. Chip manufactures seem to have reached a stagnant point that shifted a high market share towards optimization. However, after some experience, raw performance optimization has also been deemed as not profitable enough. As a result, novel ICT products and services are shifting towards a data-oriented model, where the information gathered takes the main role. In this regard, companies and institutions are taking a deep look into *what* can actually be achieved with the available hardware chips and devices [38]. This has been denominated as the *maker's movement*.

IoT device heterogeneity not only refers to hardware and computational specifications, but also to the transmission needs of end-devices. There is a heterogeneous networking characterization of end-devices in terms of: (i) the requirement of transmissions of large or small packets, (ii), the transmission frequency, (iii) how delay-tolerant the communications are, e.g., the possibility of bulk transmissions like large amounts of data, and (iv) how *important* is the end-device. The device importance in this context refers to how critical is the successful transmission of data from or towards that entity, e.g., remotely activating a firefighting sprinkler valve has preference over turning on a street light-post. This becomes a new factor to take into consideration with regards to network capacity and scalability.

Also, it is reasonable to think that IoT is a key enabling technology tightly attached to the advancement of cloud, edge, and fog computing. Solutions that benefit from the coordination and management of massive and heterogeneous device deployments have demonstrated their capacity to solve complex problems [39]. As more advantages are found in these computing solutions, the drive to

improve communication technologies increases in the realm of IoT.

The purpose if this chapter is to give a contextualized and cohesive summary of the research conducted during this PhD thesis period. It offers a better sense of the research gap that motivated it, and the research proposals offered in order to fill that breach. The remainder is organized as follows. Section 3.1 shows a summarized analysis of the current communication challenges of IoT over low-power networks. In Section 3.2, the state-of-the-art related work techniques are reviewed and summarized for the secure and authenticated integration in the IoT paradigm of embedded devices communicating over low-power radio technologies, based on the challenges and gaps described in the previous section. Section 3.3 presents the research proposal framework for the communication of IPv6/UDP/CoAP packets over low-power long-range communication technologies by using a novel header compression and fragmentation mechanism. In addition, it presents a lightweight authentication and key agreement mechanism that ensures a secure and private communication. Finally, Section 3.4 shows the conclusions and lessons learned during this research period.

3.1. Low-Power IoT Communication Challenges

Thanks to the benefits brough by the IoT paradigm, novel products and services are achieved in different areas and applications. As a consequence, the IoT paradigm drives a high grade of heterogeneity among the different devices and hardware employed across the increasing number of available solutions. One of the most direct ways to categorize IoT-based projects is by the employed hardware or devices used in the deployment. Certain scenarios may require the deployment of hundreds, or even thousands of devices in sparse geographical areas, that typically lack power-grids or wired connectivity. These kinds of scenarios are commonly present in applications within the scope of Smart Cities, Smart Agriculture, and Industry 4.0.

To solve this issue, these scenarios rely on the deployment of low-power devices running a micro-controller system-on-chip (MCU SoC) that integrates a set of electromechanic sensors and actuators. Together, they may include communication modules such as radio transceivers or GPS receivers.

This kind of devices receive many different terms and denominations, from embedded systems, to *Arduino-like* devices. However, a more technical definition was achieved by the Internet Engineering Task Force (IETF) in terms of computational power and characteristics. This definition is presented in RFC7228 [40], where the term employed is *constrained devices*. Furthermore, they typically have a small form factor — with a size similar to a matchbox — transmit a few packets each day, and are installed in hard-to-reach locations. They are intended to work autonomously, oftentimes operating under extreme or harsh conditions — e.g., sensor devices installed outdoors subject to climate conditions, buried under a layer of asphalt for traffic monitoring, inside freezers for sanitary control applications, or in waste sewer systems for pest control, among others.

As a consequence, IoT introduces constrained devices with different characteristics. They posses different life-cycles, that can range from a few months, up to several years. Generally, they lack keypads or displays, as their intended purpose is to operate in an unsupervised fashion without human interaction, besides the installation itself. Additionally, due to their relatively long life-spans, of several years, they can switch administrative owner several times during this period, and do not present an scalable way to reprogram the code.

3.1.1. Low-Power Wide Area Networks (LPWANs)

The explosion of the massive IoT paradigm presents a large amount of challenges that need to be addressed in the near future. One of these challenges is related to the connectivity in use cases where up to thousands of devices within a same network transmit packets at sporadic hours thorough the day. One of the solutions that have partially filled this gap are Low-Power Wide Area Networks (LPWANs) [8]–[14]. One of their main advantages is to provide connectivity to large coverage areas with a reduced amount of base stations. LPWANs operate by employing long-range radio transmission

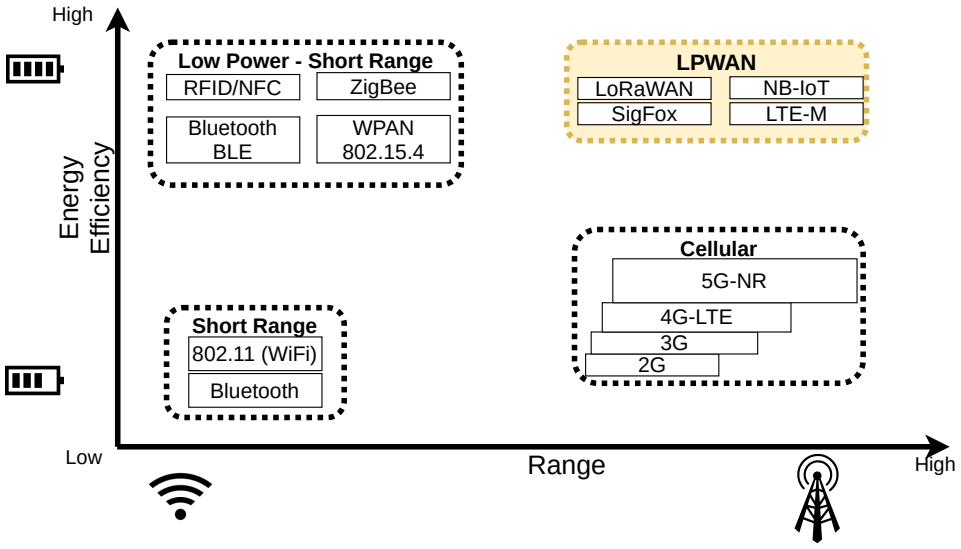

Figure 3.1: Radio access technologies classified by energy efficiency and coverage range.

technologies and modulation techniques with a focus on distance, cost of device, and energy efficiency. Fig. 3.1 shows a classification of radio access technologies by energy efficiency and coverage range. LPWANs allow the connectivity of remote rural regions without dense cellular connectivity, i.e., it provides an affordable connectivity solution to areas lacking 4G or 5G base-stations. Due to the lack of power-grids, LPWANs also prioritize the aggregated energy consumption of all the end-devices as a key performance factor in their design and approach. Lastly, another relevant performance metric when evaluating LPWAN solutions is their interference susceptibility when simultaneous communications take place in co-channels [13]. However, these notable characteristics are attained at the expense of having a highly constrained communication channel. Some of the most common LPWAN technologies are: Sigfox [16], LoRaWAN [17], Narrowband-IoT (NB-IoT) [18]–[22], Long Term Evolution for Machines (LTE-M) [10], Weightless[1], and Ingenu's Machine Network[2].

LPWANs highly constrained communication channel is designed to support a limited number of short packets per device per hour. These technologies can be broadly categorized by the kind of radio band employed in the transmissions. On the one hand, LPWAN technologies can employ licensed radio bands. In these technologies, the end-user pays a monthly fee to the service provider, granting the user a certain level of Quality-of-Service (QoS) achieved by reserving part of the radio spectrum to the client. This approach is commonly undesirable due to the subscription fee severely increasing cost-per-device. On the other hand, LPWANs can use unlicensed radio bands — e.g., the Industrial, Scientific and Medical (ISM) band, a part of the radio spectrum that is reserved in most countries to be employed for these purposes without paying a fee. In order to achieve a smaller cost-per-device, unlicensed radio bands are popular among LPWANs. However, guaranteeing a certain QoS level is considered as a killer feature in any LPWAN that can achieve it. This QoS level is easy to obtain in a licensed radio band, due to the control over the interference. By contrast, sharing the medium among different technologies makes achieving a minimum QoS level in unlicensed radio bands a complex problem. As an illustration, the maximum transmission power in licensed radio bands is notably higher than in unlicensed radio bands — e.g., 23 dBm vs. 14 dBm for licensed and unlicensed radio bands in Europe, respectively. Also, these regulations imposed on unlicensed radio bands have an impact on the maximum amount of data each device is permitted to transmit. Specifically in the case of the 868

[1] http://www.weightless.org/
[2] http://www.ingenu.com/

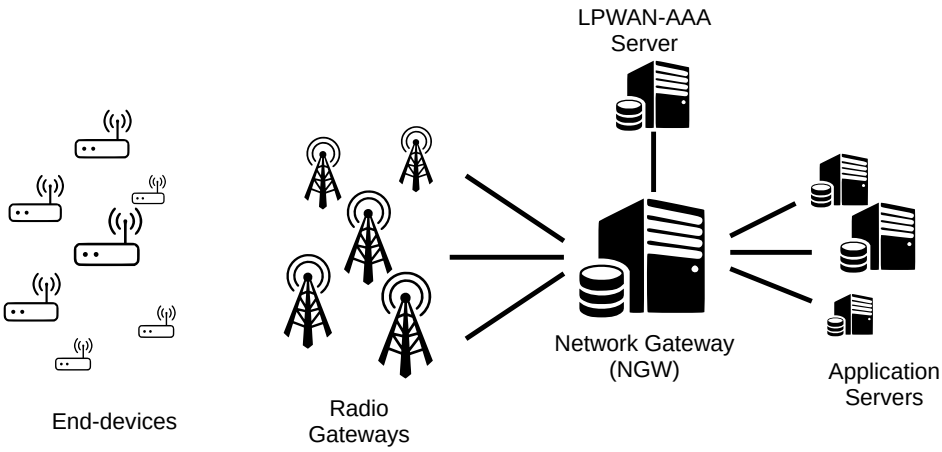

Figure 3.2: LPWAN generic architecture framework according to RFC8376 [9]

MHz ISM radio-band in Europe, each device is permitted to transmit up to 36 seconds per hour, also known as duty-cycle [41]. Thus, choosing licensed over unlicensed radio bands is a decision that must be carefully studied and opted only if the use case explicitly requires a higher QoS grade.

LPWANs share common traits in their architecture and components. These have been identified in [9]. They form a star-of-stars topology, as shown in Fig. 3.2. Devices communicate exclusively with radio gateways over a constrained radio technology. In turn, the radio gateways rely all the received messages back to a central network gateway that manages the whole network. This approach greatly saves complexity at end-devices, pushing it to the non-constrained network infrastructure. For instance, the end-devices do not form mesh networks, omitting all the stateful routing and forwarding logic. Additionally, since all the transmitting devices, eventually reach the network gateway, there is no need for a networking layer either. All of the aforementioned characteristics make LPWANs an attractive solution for large sensor deployments [42]. Radio gateways are connected through a non-constrained backhaul link to the network gateway, such as Ethernet or 4G. The network gateway is in charge of delivering each received message from the network to the corresponding application server. Application servers presents a developer-friendly abstraction of several end-devices. They hide the details of the underlying networking processes and simply act as an API. Please note that application servers do not run the customer logic, they simply present an end-point for customer dashboards or database agents for the business logic in a friendly form. To achieve this, the technology employed by each LPWAN is vendor-specific and tailored to the deployment — e.g., HTTP RESTful API, MQTT, CoAP. The LPWAN network gateway also manages overall connectivity monitoring and the de-duplication of received messages. Typically, a platform dashboard is presented to the network operators to monitor and analyze the status of the network. Lastly, the LPWAN-AAA server manages the authentication process that devices perform to access the network. Typically, the network gateway and LPWAN-AAA server are co-located in the same host.

Security and privacy is currently an ongoing challenge in every LPWAN-based scenario. LPWANs generally have a tendency for fewer protocol layers. This is because each protocol stacked on top of the constrained radio link introduces extra headers and increase the packet overhead. For this reason, LPWANs typically employ vendor-locking security mechanisms that lowers the much desired interoperability envisioned by the IoT paradigm [43]. As a consequence, devices connected through a specific LPWAN technology from isolated connectivity islands that prevent them to address other devices connected to the Internet. Due to the severely bandwidth limitations encompassing LPWANs, confidentiality and privacy methodologies that exchange packets larger than a few 10s or 100s bytes are prohibitively expensive. For this very reason, commonly employed security protocols employed today in the Internet are not reused in LPWAN solutions. LPWANs also prefer shorter packet sizes to avoid

fragmentation. Large security related messages that need to be fragmented present an undesirable effect because it creates new attack vectors for state-exhaustion attacks [26].

LPWANs are even more constrained regarding bandwidth than other established low-power solutions, as those employed in market ready WSN solutions. For instance, the design and trade-offs of low-power short-range communication technologies, such as those based in IEEE 802.15.4 radio technologies, must be considered as a different networking class. Even severely constrained security mechanisms used in those may not be apt for their use in LPWANS.

Another shortcoming of LPWAN technologies is their lack of mechanisms to securely access third-party domains. This is, that end-devices do not have the capability to securely access end-points beyond the LPWAN deployment itself. As a result, the LPWAN mechanisms shipped with each technology assume a total trust in the confidentiality and privacy management of the transmitted information.

In an attempt to reduce some of the aforementioned challenges, some LPWANs implement federation options to merge existing deployments, previously owned by different administrative domains — e.g., if two different companies are merged into one, they may also merge the massive sensor deployment. However, these mechanisms are tightly coupled with the technology and employ tailored protocols that do not grant interoperability with networks from other vendors.

3.1.2. Security Challenges in Low-Power Communication Technologies

Security in massive IoT scenarios must be carefully studied at the design state, before the final deployment of the devices. Due to the aforementioned deployment cost and characterization of LPWAN use cases, fixing a software bug or code vulnerability has a prominent complexity and a potential prohibitive cost. Since all the deployed devices must be updated with the new version of the code, this becomes a time-consumption procedure, that forces an operator to be present at each location. If the device does not present a connection port — e.g., devices installed under a layer of asphalt — the cost increases even more.

In this regard, it is a popular suggestion for massive IoT deployments that design and development stages are approached by thinking that the device will eventually be *installed in another planet*. This is a succinct way to express the potential failure of a deployment in case of requiring firmware code updates. Being able to transmit to remotely and wirelessly transmit firmware binary code over radio is still an ongoing challenge for LPWANs, due to bandwidth limitations. This technology is known as Firmware Over the Air (FOTA), where a binary image of the operation code is distributed to end-devices through radio. However, popular LPWANs using unlicensed radio bands do not implement FOTA procedures within their specification. Additionally, security in FOTA procedures is a major concern due to potentially exposing proprietary code, resulting in severe business losses. Besides, it stands to reason that some firmware codes may embed cryptographic material required to exploit third party storage solutions hosted in the cloud, such as Amazon Web Services (AWS) or Microsoft's Azure. Obtaining a copy of the firmware could mean access to these cloud storage solutions, potentially holding private data from the network operator.

Developing both interoperability and security in massive IoT scenarios is currently a challenge in the road-map to obtain interoperable large scale deployments in next generation applications [125]. Massive IoT scenarios revolve around improving the cost per device, in turn making their logic simpler and more predictable. Hence, this turns IoT devices into a high priority target for Distributed Denial-of-Service (DDoS) attacks. These deployments must be supported by the rest of the infrastructure, requiring vast amounts of processing power and storage solutions.

Furthermore, trustworthy confidentiality and privacy is not only a desirable feature, but also has been expressed as one of the key society's concerns when employing the IoT paradigm. As such, IoT technologies must gather the public's trust and abide by the laws present in each region. For instance, in the European Union, there is a set of regulations that compose the foundation regarding cybersecurity privacy and confidentiality, namely, (i) the Network and Information Security (NIS) Directive for internetwork operation [44], (ii) the european General Data Protection Regulation [45],

(iii) and the European Union Agency for Cybersecurity (ENISA) ICT cibersecurity certification [46].

3.2. Related Work

There is a need for a coordinated and comprehensive effort where all the parts in an IoT ecosystem collaborate in order to enable LPWAN interoperation [43]. This is needed to future-proof all the technologies leveraging on current LPWANs. A determining factor in this pursuit are open protocols.

Ongoing research regarding the integration of secure protocols for IoT scenarios leveraging on low-power communication technologies can be broadly categorized in two different parts. On the one hand, research is conducted to solve and engineer connectivity aspects of low-power communication technologies. This encompasses reducing the frequency and overall length of the transfer packets, while maintaining an scalable and cost-effective massive IoT scenario. On the other hand, additional research is also conducted in order to provide confidentiality and privacy using lightweight cryptographic suited for constrained devices.

Energy efficiency is the most relevant key performance metric in order to validate research proposals for massive IoT scenarios relying on LPWANs [8], [42], [47]–[50], [120]. End-devices spend most of the time in a low-power consumption mode, known as *sleep mode*, and only switch out to periodically transmit sensor data or when an event happens. At sleep mode, constrained devices drain electrical current in the order of µA. Furthermore, common MCU models allow switching to an even more energy efficient mode, known as *deep-sleep mode*, draining current in the order of a few nA. By comparison, when the device is required to transmit data, the MCU needs switches back to an active mode that drains current in the order of a few mA, in addtion to activating the radio transceiver, which consumes relatively large amounts of energy. Common LPWAN solutions have maximum transmission power limitation values ranging from 14 and 23 dBm. At a nominal voltage value of 5V, this equates a current drainage between 5 and 40 mA, respectively. As a consequence, when transmitting information, the current usage of the constrained device can be up to 7 orders or magnitude higher than while waiting for an event or a timer to expire.

Regarding extending the battery life of end-devices, research can roughly be categorized in two different areas, namely, Energy harvesting techniques, and decreasing consumption [47]. Typically, there is a preference for the later, due to the undesirable extra cost of adding energy harvesters to a massive IoT scenario.

3.2.1. Internet Protocols and Low-Power communication Technologies

The IETF is the standardization organization in charge of Internet protocols. These protocols are open and free to use without license, aimed at fostering industry interoperable and future-proof deployments that can be managed and maintained, even if the original vendor stops supporting their solution. The IETF standardization tasks are grouped in different Working Groups (WG), in charge of different areas of interest. Due to the continuous growth and relevance of IoT solutions, the IETF has assigned several resources to study the challenges found when enabling IoT use cases over low-power communication technologies. A summary of the most relevant IETF WGs related to IoT security challenges and communication technologies can be found in RFC8576 [26]. Some of the more noticeable working groups are highlighted as follows.

- *6lo* WG[3] is in change of enabling the transmission of IPv6 packets over low-power technologies such as those based in IEEE 802.15.4 — typically employed in short-range low-power networks — or Near Field Communication (NFC), among others.
- *6LoWPAN* WG[4] has defined lightweight protocols for the transmission of IPv6 packets over low rate wireless personal area networks (LR-WPANs), RFC4919 [27]. Please note that many

[3]https://datatracker.ietf.org/wg/6lo/about/
[4]https://datatracker.ietf.org/wg/6lowpan/about/

of the protocols defined by the 6LoWPAN WG have been the main inspiration for numerous research proposals trying to achieve efficient methodologies in LPWANs. Protocols standardized by 6LoWPAN WG are a widely used baseline when analyzing the performance of novel solutions.

- *CoRe* WG[5] is in charge of the standardization of RESTful enabling protocols within constrained devices. Their main contribution is the widespread Constrained Application Protocol (CoAP) [25]. It enables a web-based interaction centered around the access to resources hosted in an end-device — analogous to HTTP.
- *LPWAN* WG[6] defines efficient mechanisms to implement IP-based protocols over LPWANs. Their most significant contribution is Static Context Header Compression (SCHC) RFC8724 [15]. It is a mechanism that allows the transmission of IPv6/UDP packets over an LPWAN through header compression and fragmentation.
- *LWIG* WG[7] collects the experiences of light-weight implementations of IP stacks in constrained devices and networks. It provides guidance documentation on how different protocols or mechanisms should be implemented in MCUs.
- *T2TRG* WG[8] is in charge of Thing-to-Thing research. It focuses on how heterogeneous constrained devices can address and interact directly with other constrained or non-constrained devices running rich operative systems such as Windows, macOS, or Linux. This initiative tries to materialize the IoT vision of all end-devices communicating over the network, regardless or their characteristics or computational capacities.
- *ACE* WG[9] establishes mechanisms to allow only authenticated and authorized access to resources hosted on constrained environments.

The standards created by the aforementioned IETF WGs have become the baseline for many other standardization efforts, not only within the IETF, but also for different organizations focused in IoT scenarios. Some of the organizations leveraging on IETF's work include: the 3rd Generation Partnership Project (3GPP)[10], Thread[11], the Industrial Internet Consortium[12], OMA SpecWorks[13], OneM2M[14], the Open Connectivity Foundation[15], Fairhair Alliance[16], and the Lightweight M2M standard (LwM2M) by OMA SpecWorks [51], [52].

The IETF WGs outlined above have a common broad vision on how information originated in constrained end-devices should be accessed and shared [26]. At the core of this vision lies a *resource*-centered paradigm, where sensor and actuation happens by accessing their corresponding resources. For instance, the `/temp` resource may refer to the device's temperature sensor reading, or writing a boolean value in the `/window-latch` resource encompasses the device opening or locking a window frame latch. All of these resources are addressable by a Unique Resource Identifier (URI) — e.g., `coap://2001::1/temp` — allowing secure and authenticated web-based request-and-answer interactions. The IETF broadly categorizes the protocol families in two different groups. On the one hand, there are protocols and mechanisms in the data transmission plane, such as CoAP, or Concise Binary Object Representation (CBOR) [53]. On the other hand, there are security mechanisms that protect the integrity and confidentiality of those exchanges. In this case, the most notable are Object

[5] https://datatracker.ietf.org/wg/core/about/
[6] https://datatracker.ietf.org/wg/lpwan/about/
[7] https://datatracker.ietf.org/wg/lwig/about/
[8] https://datatracker.ietf.org/rg/t2trg/about/
[9] https://datatracker.ietf.org/wg/ace/about/
[10] http://www.3gpp.org/
[11] http://threadgroup.org
[12] http://www.iiconsortium.org
[13] http://www.omaspecworks.org/ipso-alliance
[14] http://www.onem2m.org
[15] http://openconnectivity.org/
[16] http://www.fairhair-alliance.org/

Security for Constrained RESTful Environments (OSCORE) [54], and Datagram Transport Layer Security (DTLS) v1.3 [55].

For the data transmission plane, considering both the target scenario conditions and the need for a web-based interaction, the IPv6/UDP/CoAP stack has been introduced as a fundamental building block of an homogeneous and interoperable secure IoT ecosystem [26]. Due to the continuously growing number of connected devices, the IPv6 [56] address space is required, as opposed to the arguably exhausted IPv4 alternative. Also, constrained networks transmit single units of data in short packets of 10s or 100s of bytes. In battery-powered scenarios, stream-based communications are prohibitively expensive and inefficient when transmitting small units of data at sporadic times of the day. As a consequence, UDP has been chosen over TCP as the transport layer thanks to its simplicity and feature set trade-off. Since networks and devices are likely to operate over lossy communication technologies, radio re-transmissions and delayed responses are likely to occur. To support a web-based interaction considering these conditions, the IETF has envisioned CoAP as the centerpiece of the framework. Like HTTP, CoAP allows RESTful operations on resources, such as GET, POST, UPDATE, or DELETE, while the secure protocols guarantee a controlled access.

In non-constrained environments, for all the web-based interactions, JavaScript Object Notation (JSON) [57] has become the common solution for transmitting structured schema-less application-level data. However, the transmission of JSON messages over constrained environments has been deemed as inefficient. To fill this gap, the CBOR protocol is employed instead, requiring significantly shorter packets than JSON in IoT use cases. Consequently, while HTTP/JSON has become the defacto standard in non-constrained environments, the IETF states that the CoAP/CBOR is expected to be integrated in future IoT applications. Furthermore, the integration of constrained systems is facilitated by using CoAP/CBOR to HTTP/JSON proxies that translate the packet units from one scheme to another. The IETF has stated that this type of proxy is easily implemented [26] and does not impose any kind of sacrifice or overhead in the constrained side of the deployment once integrated. Besides, CoAP and CBOR are protocols specifically designed with MCU-based constrained environments in mind. As a consequence, they are relatively easy to implement in low-level languages like C or assembly, and occupy smaller binary code footprint compared to their non-constrained counterparts. Also, in order to avoid unnecessary network transmissions, these protocols do not have several available versions and avoid radio transmissions that negotiate sets of features or versions. Due to all the aforementioned advantages of CoAP and CBOR, the IETF expects their wide-spread availability in the form of libraries in the main embedded software development kits and frameworks, such as ArduinoIDE[17], or ARM Mbed[18].

Regarding confidentiality and privacy, the IETF has defined an extensive set of diverse and heterogeneous use cases for IoT environments where authentication and key agreement mechanisms are required. These use cases are described in RFC7744 [58], where CoAP is established as an enabling technology, while other generic alternatives might fit the part. In order to provide security to the CoAP application level data, OSCORE in conjunction with CBOR Object Signing and Encryption (COSE) [59] offer a solution with low performance impact thanks to their header overhead of 11–13 bytes [60]. OSCORE only protects the application payload that contains the relevant resource. Thus, request-response exchanges can be protected regardless of the underlying technology being employed during transport, even through non-IP networks. This is thanks to intermediate proxies and routing components having access to the CoAP header fields in plain-text, which allows almost direct CoAP-HTTP agents.

3.2.2. Transmission of IPv6 packets over Low-Power communication technologies

As aforementioned in Section 3.1.1, the IoT brings together heterogeneous devices and technologies. Some of these devices are expected to run for several years, which could mean that the original manufacturer might go out of business and stop giving proper support and maintenance updates.

[17] http://www.arduino.cc/en/software
[18] https://os.mbed.com/

Hence, in order to guarantee long-term end-device operation, deployments must be future-proof. Thus, the integration of several LPWANs through open standardized Internet protocols is the key enabler to materialize the original IoT vision of massive deployments. Also, this would allow devices to interact with other machines or deployments outside their LPWAN domain.

The problem of transmitting IPv6 packets over low-power long-range communication technologies has been previously explored. Typically, in its earlier stages, technologies related to the 6LoWPAN ecosystem were studied as a baseline due to their relative similarity to the limitations and use cases of LPWANs. The authors of [61] tried to implement an exact copy of the 6LoWPAN network stack, but instead of using an IEEE 802.15.4-based physical radio chip, they employed LoRa modules instead. Another different approximation was presented in [62], where the regular LoRaWAN network architecture is supported, in addition to customized IPv6 packets that use a different LoRa format. The radio gateway is modified to identify these customized IPv6 packets. Hence, when a regular LoRaWAN message is received, it is forwarded to the central network gateway. Otherwise, if a customized IPv6 packet is detected, it is forwarded directly to the Internet, without employing the rest of the LoRaWAN architecture. Additionally, the authors of [63], [64] implemented and evaluated the transmission of IPv6/ICMPv6 packets using a scheme inspired in SCHC over LoRa radio transceivers.

However, it is worth to point out that all the aforementioned research proposals to transmit IPv6 over low-power long-range technologies have a common drawback, namely, all require the explicit modification of each participating radio gateway. This approach is arguably not scalable in terms of operation and maintenance of massive IoT scenarios. While radio gateways are not constrained devices themselves, they include tailored hardware and software that interfaces with the transceiver and forwards messages to the central network gateway. Furthermore, radio gateways may belong to a different administrative domain, outside of the operator reach, denying these proposals. Furthermore, each LPWAN radio gateway potentially serves thousands of end-devices, thanks to their project large coverage range, of tens of kilometers. Thus, the customized software required to enable the aforementioned approaches must be analyzed and evaluated in order to avoid computational bottlenecks. In order to foster interoperable and scalable solution, alternatives that follow the LPWAN star-of-stars topology are preferred.

The IETF LPWAN WG plays a relevant part in the integration of devices that have connectivity through different LPWAN flavors. The need to homogenize as many common LPWAN aspects as possible has already been identified [9], [51], [52], [54], [65], [66]. LPWAN techs mostly rely on simple network stacks where application data is directly carried at the MAC layer. This is a contradiction of the IoT paradigm, where IP-based protocols and architectures are employed as a common ground to enable the seamless interaction of devices belonging to different deployments.

Due to the massive scale of IoT devices, the IPv6 address space is necessary. However, the IPv6 protocol includes a mandatory header that is 40 bytes in length. This is prohibitively expensive in LPWAN scenarios, where the typical packet lengths range from 10s to a few 100s of bytes. Furthermore, some LPWANs, like Sigfox [16], have a maximum data sizes smaller than the size of the IPv6 headers alone.

In order to allow the transmission of the IPv6 messages over LPWAN technologies, the IETF LPWAN WG has standardized the Static Context Header Compression (SCHC) RFC8724 [15]. It is a novel mechanism that provides a header compression and optional fragmentation for IPv6/UDP packets. Through this header compression, a higher level of efficiency is gained by constrained devices for accessing the Internet. Additionally, the SCHC mechanisms can be extended with mechanisms that further compress higher stack layers. Specifically, the SCHC can be employed to compress CoAP headers [67]. Although CoAP is considered as a constrained protocol, with low-power networks and devices in mind, still its headers are considered as too large for LPWANs. Thus, when applying both mechanisms, the IPv6/UDP/CoAP stack headers can be compressed.

Overall, SCHC's biggest contribution is its capacity to hide the underlying LPWAN specifics and architecture. Instead, connected devices can be seamlessly integrated through IP-based architectures, such as the Internet, granting them the capacity of being addressable through IPv6. SCHC introduces a seamless adaptation layer between IPv6 and the underlying LPWAN technology, as shown in Fig. 3.3.a.

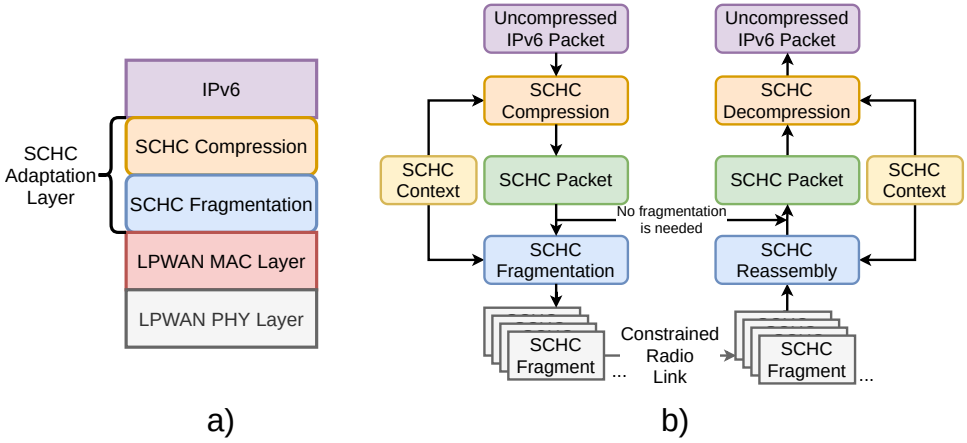

Figure 3.3: (a) SCHC adaptation layer within in the network stack. (b) SCHC compression and fragmentation data flow.

SCHC exploits certain characteristics of LPWANs in order to perform efficient header compression. On the one hand, the star-topology of LPWAN guarantees that the source-destination path does not change. As a result, if components of the back-haul, like radio gateways or network gateways, need to change their network address or routing paths, this does not affect the successful packet delivery. On the other hand, embedded firmwares are not likely to change drastically during the device lifetime. Hence, the traffic flows of the target deployment are well-known in advance.

SCHC operation is split in two different modules, namely, compression and fragmentation, as shown in Fig. 3.3.b. First, whenever a new uncompressed IPv6 packet reaches the SCHC compression module, it attempts to compress the headers with the best possible compression ratio. Either if the compression affected its size or not, the product of this step is named *SCHC Packet*. Next, if the maximum packet length threshold is reached, the underlying optional fragmentation step is applied. In order to extract the original packet, the inverse process is applied on the receiving end. To this end, SCHC stores the information regarding how the IPv6/UDP/CoAP header compression and decompression must be performed in a *context*, which is composed by a list of *rules* in turn. Each rule represents one flow of information — e.g., reporting the data collected by a sensor using a CoAP POST method to a cloud component can be expressed as a *context rule*. During the compression step, all the available rules in the context are evaluated, and the one that provides the better compression ratio is chosen to be applied. As a result, the first bits of data in SCHC packets contain a mandatory field name *Rule ID*. Its purpose is to tell the other end-point what rule should specifically be applied when decompressing the packet. The standard does not define a fixed Rule ID field length, it depends on the underlying LPWAN technology and the size of the context. Commonly the Rule ID takes an octet of the SCHC packet. After the Rule ID, the header-related data that could not be compressed is appended to the packet, known as SCHC compression residue. Finally, the remainder of the produced packet contains the payload of the original uncompressed IPv6 datagram.

There are other existing solutions for header compression focused on scenarios with scarce network resources. Header compression mechanisms commonly found in low-power technologies can be broadly categorized in two different classes, as shown at the top of Fig. 3.4. On the one hand, there are stateful header compression mechanisms — e.g., Robust Header Compression (RoHC) RFC5795 [28], and the compression format for IPv6 datagrams over IEEE 802.14.4 networks (LOWPAN_NHC and LOWPAN_IPHC) RFC6282 [29]. They require the exchange of context-building packets, known as signalling, before being able to transmit user payload data. These mechanisms typically achieve better compression results at the expense of adding extra overhead to the communication. On the other hand, there are stateless header compression technologies, capable of transmitting compressed payload data

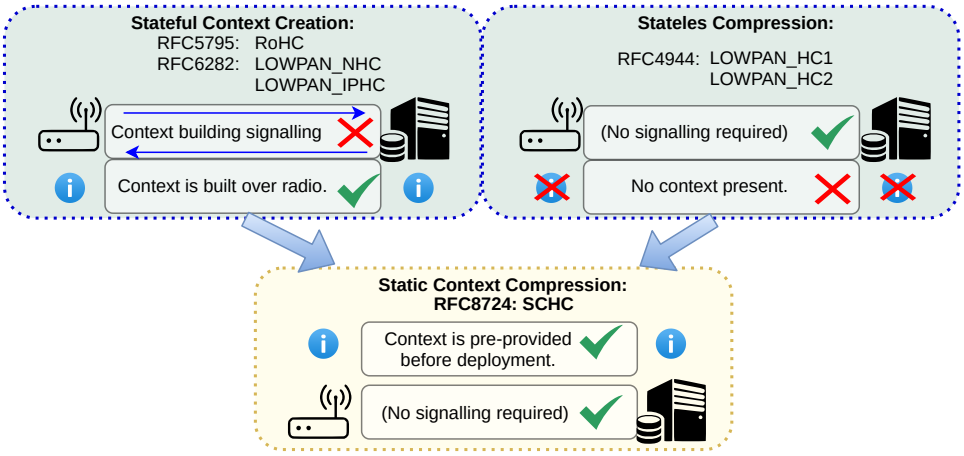

Figure 3.4: Categorization of state-of-the-art header compression mechanisms for low-power networks.

without any previous context — e.g., LOWPAN_HC1 and LOWPAN_HC2 RFC4944 [30]. This way, stateless compression mechanisms save radio spectrum usage, battery life, and binary code footprint. However, these techniques may have difficulties when facing random traffic flows, yielding worse results.

However, SCHC innovation sets itself apart from other solutions by exploiting the best advantages of both categories, i.e., SCHC benefits from having a context without requiring the signalling process, as shown in Fig. 3.4. This is, SCHC does not require context building signalling, its context is static and unique. This is possible thanks to the predictability of the device's operation code and data flows, the context is designed and pre-provided to the device before it is deployed.

SCHC is independent from the supporting LPWAN technology below it. Since not all LPWAN technologies include a Maximum Transmission Unit (MTU) large enough to fit the mandatory maximum 1280 bytes of IPv6 [56], SCHC presents an optional frgamentation procedure tailored to LPWAN's low datarate requirements. Additionally, SCHC is generic and offers several configurable parameters to tailor the mechanism to the specific needs of the deployment. For instance, the fragment size for large IPv6 packets can be chosen, based on the low-power radio technology employed. There are several use cases where SCHC might be applied to higher communication layers. Specifically, in the case of compressing protocols with large amounts of serialization that include a length field prefix that announces the length of the following fields, or the number of times a field appears. All of these aspects can be passed on to an SCHC context.

To achieve the high compression ratio, the SCHC context *stores* field data for known traffic flows. If a header field is expected to always have the same value for a certain flow, it is stored in the context as a *target value (TV)* [15], and tagged as *not sent*. To illustrate this, if the UDP listening port for one end of the communication is always the same, e.g., 5863, this value gets stored in the context. As a consequence, it is never sent over the constrained radio link. Hence, the most frequent traffic flows are well known in advance, and will save the transmission of redundant header fields whenever possible.

The performance of SCHC compression has been evaluated in [68]–[72], [120]. These works conclude that SCHC is a promising technology for the transmission of IPv6 packets over LPWAN as it outperforms other state-of-the-art strategies. As aforementioned, LOWPAN_HC1 and LOWPAN_HC2 (RFC4944) [30] are stateless mechanisms for the compression of the network and transport layer protocols, respectively. They can compress the IPv6 header and UDP header to two and for bytes, respectively. However, please note that this maximum compression ratio can be obtained only when compressing link-local addresses. This standard got a new upgrade in RFC6282 [29], which further improves the header compression proposed in RFC4944. These mechanisms are defined as LOWPAN_IPHC and LOWPAN_NHC for the network and transport layer protocols, respectively. Nevertheless, it requires a stateful context creation that requires the transmission of signalling packets,

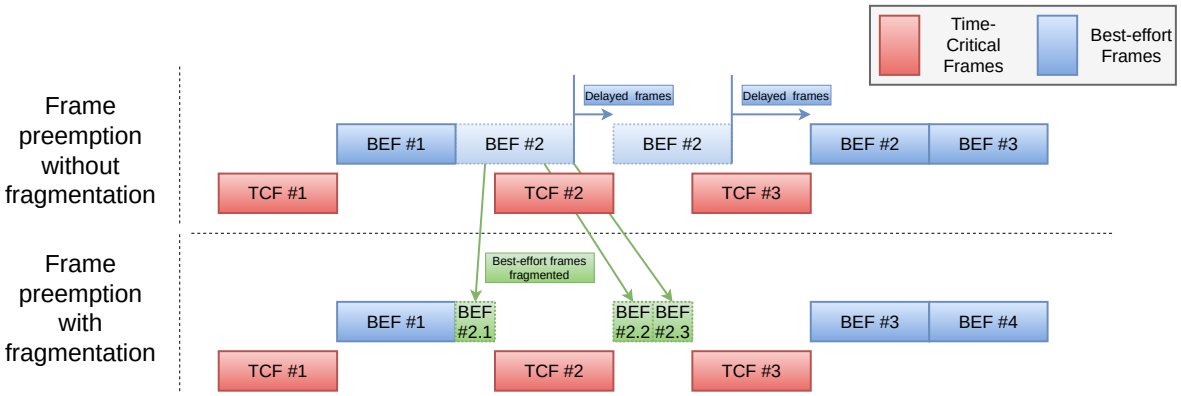

Figure 3.5: Frame preemption concept in the context of packet fragmentation

costing a higher amount of bandwidth and battery power per traffic flow. The signalling overhead of LOWPAN_IPHC and LOWPAN_NHC can be as low as ten bytes in the best case scenario [69]. Please note that this signalling exchange also includes the corresponding underlying LPWAN header overhead — this makes the overhead significantly higher than ten bytes in the best case scenario. Nevertheless, SCHC is able to achieve a header compression resulting in one single byte for the whole IPv6 and UDP headers — please refer to the Appendix A of [15] to see compression examples that achieve this feat.

In order to support the relatively large IPv6 MTU of 1280 bytes, 6LoWPAN [27] employs an adaptation layer that defines a simple fragmentation mechanism without reliability [30]. This fragmentation scheme employs a timer that expires after not receiving new fragments for a period of sixty seconds. When that happens, the buffered fragments are discarded. RFC6282 does not modify nor improves this fragmentation mechanism. The impact of 6LoWPAN fragmentation has been evaluated in [73], where the authors studied the performance of different routing protocols in a real-life 6LoWPAN scenarios. The work concludes that fragmentation avoids retransmissions, thus introducing an overall performance improvement. Furthermore, work in [74] states that 6LoWPAN compression together with its fragmentation mechanism can extend end-devices battery-life up to a 3% due to header reduction.

As opposed to 6LoWPAN lacking a fragmentation reliability mechanism, SCHC implements three different reliability modes, namely, No-ACK, ACK-Always, and ACK-on-Error. These modes accommodate different channel conditions regarding channel directionallity and error rates. The SCHC fragmentation mechanism is an optional step that only takes place when the compressed SCHC packet is deemed too large for the LPWAN technology employed. Each SCHC packet is split in several SCHC fragments payloads, as illustrated in Fig. 3.6. Please note that each SCHC fragment includes an extra overhead of fragment headers that must be taken into consideration. The fragmentation trade-off is a problem evaluated in [120], where choosing the SCHC fragment size can have repercussions on the overall network's performance and must be tailored to the deployment's needs.

After evaluating the performance of several fragmentation schemes in [75], [76], [120], they conclude that some scenarios may benefit from reducing the fragment size, even if the original packets fit within the LPWAN's maximum packet size. This way, the transmission throughput converges to a certain rate depending on several radio channel conditions. Once that throughput value has converged, further reducing the fragment size may worsen the throughput, due to the header size overhead introduced by the underlying LPWAN technology. This is, each deployment must be studied to find the optimal fragment size value.

One of the advantages of fragmentation over LPWANs is that, it may improve the overall performance of *Frame preemption*. Frame preemption is a generic concept, mainly borrowed from IEEE 802.1Qbu standardization [77] to provide certain QoS features to LPWAN-based IoT transmissions. It can be implemented with and without frame fragmentation, as shown in Fig. 3.5. Frame preemption adds

another dimension to the transmission of LPWAN messages. It categorizes packets with regards to how timely their delivery must be. On the one hand, time-critical frames are those queued elements with an specific delivery deadline or asynchronous events that must be sent as soon as possible, like a fire alarm. On the other hand, best-effort frames are packets that must be transmitted as soon as possible but do not have an established deadline, e.g., a periodic sensor data measure. First, the transmitter's scheduler will try to fill the channel with time-critical frames, next, it will fill the remaining time slots with best-effort frames (Fig. 3.5). However, if an asynchronous event triggers the transmission of a time-critical frame, like an alarm, it interrupts any other communication and sends the new time-critical frame instead. Once the channel is free again, the transmission of the previously interrupted best-effort frame gets resumed. Thus, frame preemption is a behaviour found in many different communication domains, but in the context of low-power networks, the re-transmission of relatively long packets encompasses a high overhead due to the aggregated cost of each interrupted best-effort message.

In order to address this issue, fragmentation can be applied in the context of frame preemption to allow queuing smaller units in the remaining time slots, attaining a more efficient use of the channel. Splitting best-effort frames into smaller units, reduces the number of re-transmissions required when asynchronous events occur. Since frame preemption is not considered within the different LPWAN technologies, SCHC fragmentation may improve their feature set by enabling an efficient bandwidth usage in this context.

Nevertheless, there are some identified drawbacks in the way that SCHC operates. First, it has been identified that the standardized SCHC can be applied only per LPWAN deployment, which forces installing a SCHC compression and fragmentation module on each LPWAN's network gateway — please see Fig. 3.2. This is, the integration in cross-LPWAN deployments is left out of the RFC's scope. To address this, Moons *et al.* [69] propose a multi-modal LPWAN architecture where the same SCHC compression can be employed in cross-LPWAN deployments This is achieved through a centralized server running an MQTT server that interconnects all the participating LPWAN network gateways. This research proposal contribution is two-fold. On the one hand, it allows devices that include two different LPWAN transceivers to communicate seamlessly with the SCHC module. To illustrate this, if one device has an NB-IoT radio transceiver, in addition to a LoRaWAN one, it can employ whichever technology to carry SCHC packets seamlessly. Since all the SCHC packets will reach the same central broker, it can even switch technologies in the middle of a data transmission. On the other hand, mobile devices carrying a single LPWAN transceiver can change locations and connect to other LPWAN deployment with a different network gateway.

Another SCHC drawback is that, in order to be efficient, its design assumes that the traffic flows are predictable and well known at the development stage. If that is not the case, the static context must be loaded with several rules that will allow the device to apply the correct compression rules. Then, the context's size could grow at a fast rate. This is a concern due to the constrained storage limitations in end-devices — ranging from a few hundreds of KiBs to a couple of MiBs. This issue has been studied and evaluated in [78], where the authors presented a research proposal that reduces the context's size within the device's storage unit.

Furthermore, SCHC lacks an efficient mechanism to compress IPv6 packets when the network address is unknown beforehand. This becomes an issue if the destination host frequently changes its assigned network address. Since the SCHC context is static, there is no specific way to reflect this at the device's side. Besides, context update mechanisms are currently outside of the RFC scope. The authors of [72] presented a research proposal that addresses this issue. A pool of destination addresses is reserved for hosts that dynamically change their network address — e.g., addresses from 1 to 32. The non-constrained side of the network, has an internal mapping of each dynamic address with a domain name. For instance, if the end-device tries to target `mycloud.example.com`, it does not have to implement any domain name resolution mechanism, and simply address that entry in the context's table. On the non-constrained side of the exchange, the domain name will be resolved at the time of de-compression and use the network address instead.

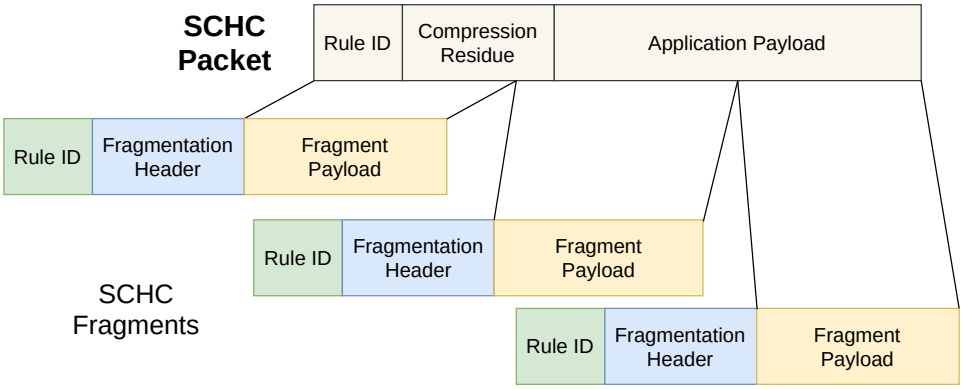

Figure 3.6: SCHC Packet and SCHC Fragment fields.

3.2.3. Authentication and Key Agreement Protocols over Low-Power communication technologies

IoT use case deployments are exposed to the common cybersecurity threats associated to scenarios where private data is exchanged in a public medium. On the one hand, confidentiality threats are associated to those attacks where the information is not accessed by the intended entity. On the other hand, integrity threats are linked to attacks where a protected data unit is maliciously captured and tampered with, in order to gain unauthorized access to other resources. The most common attacks fitting into said categories are eavesdropping and Man-in-the-Middle (MitM) attacks. Alternatively, a broader list of of attacks identified by the IETF can be found in [26]. Besides, research regarding security in low-power long-range IoT deployments typically evaluates or leverages on research proposals aimed at cellular networks due to their similarities in their security models [79], [80].

Furthermore, end-device tampering is also relevant in the context of massive IoT deployments where devices are installed in geographically sparse locations and operate without physical human supervision. For this reason, it may be also expected that an attacker may access the information stored in the flash memory within end-devices. As a consequence, security models applied to LPWANs must consider that malicious entities are able to read and write in the communication channel, as well as accessing the data stored within end-devices or network infrastructure elements, like radio gateways. Also, these models must take into consideration that attackers may be located at different points in the architecture, not only the constrained radio channel.

Whenever an end-device is installed, it performs an initial process necessary to obtain access to network infrastructure that enables the exchange of packets with the Internet. This procedure is known as *bootstrapping* and involves security operations such as authentication, key agreement, and other business logic configuration processes. The bootstrapping mechanism is of great importance to manage massive IoT scenarios in an scalable manner. In typical industrial roll-out scenarios, devices are loaded with a generic factory firmware that is not fully configured. After booting, the device accesses a remote server and downloads its specific location configuration, identified by some form of device unique tag. This configuration typically contains parameters related to the sensors and actuators, the sampling period, radio access details, or any other cryptographic material. This practice reduces management overload and allows deploying several devices with the same factory firmware in different use cases and scenarios. Also, if the operator notices during installation that the unit is faulty, it can be promptly switched with another unit without interrupting the process.

Since bootstrapping is such a common occurrence in massive low-power long-range scenarios, there is an exacerbated need to securize and standardize these operations, as opposed to using vendor-specific solutions. To address this issue, the IETF T2TRG WG presents a list of IoT security challenges and guidelines included in [26]. Furthermore, in another Internet Draft (ID) they establish that all

LPWAN technologies employ some form of previous trust relationship [81] — i.e., they are categorized as *managed* in IETF jargon. The bootstrapping procedure in LPWANs is even more bandwidth constrained than technologies commonly used in constrained low-power scenarios, such as BLE or IEEE 802.15.4-based radio access technologies. Thus, each vendor has its own ad-hoc method, with some exceptions [81], such as NB-IoT that uses the Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') [82].

Likewise, the IETF LPWAN WG also concurs in RFC8376 [9] that LPWANs should employ the Authentication, Authorization, and Accounting (AAA) framework [23], [24]. This design offers a standardized and scalable management solution for massive IoT scenarios [81] thanks to the AAA framework being an easily extensible and flexible solution fit for heterogeneous IoT scenarios. This work defines a high level security model that states what resources may or may not be accessed by different entities. The AAA framework may leverage on the Extensible Authentication Protocol (EAP) [33] and its key management framework [34]. EAP provides flexibility by being compatible with different *methods* that exchange different sets of packets and employ different cryptographic primitives. Hence, the network can employ the preferred method tailored to the deployment characteristics. This flexibility is important because low-power long-range authentication research proposals mostly rely on security protocols based in Elliptic Curve Cryptography (ECC) [83], [84] as an underlying security primitive for asymmetric keys [26]. Thanks to ECC, protocols may employ considerably smaller keys in comparison with other similar techniques. As aforementioned in Section 3.2.1, the IETF envisions the use of CoAP as an enabling technology fit for a diverse spectrum of IoT authentication and key agreement use cases [58]. A benchmark of different CoAP security protocols can be found in [85]. It compares the different mechanisms with regards to several performance parameters, e.g., message size, or number of exchanges. The protocols evaluated include DTLS v1.3 [55], OSCORE [54], and Ephemeral Diffie-Hellman Over COSE (EDHOC) [86].

3.2.4. 5G Authentication and Key Agreement for IoT Scenarios

5G systems are expected to support the authentication and key agreement of massive IoT scenarios following several resource efficiency requisites [87]–[89]. Please note that many of these requirements are tightly aligned to those identified by LPWAN technologies, as aforementioned in Section 3.1.1. As with LPWANs, 5G massive scenarios are focused on saving as much bandwidth as possible from the constrained link. As a consequence, the 5G system tries to minimize the transmission of non-user payload data, known as *signalling* in cellular networks jargon. Additionally, the medium access layers are expected to employ the least amount of protocol layers as possible in order to reduce overhead. All of these points must be achieved without hindering the mandated security requirements. Added to that, multicast communication mechanisms must be supported to efficiently transmit the same data to several devices in order to authenticate groups of IoT devices [90].

Besides, the system is expected to support private network identities, credentials, and authentication methods that are managed by a third-party administrative domain, outside of the 5G core network scope. Aligned to the IETF efforts, 5G standardization is focused on allowing bootstrapping in constrained networks and devices. Likewise, 5G is also expected to avoid relying on vendor-locking solutions, in favor of interoperable and openly standardized technologies. For these reasons, the internal 5G authentication procedures rely on EAP-based authentication and key agreement mechanisms, e.g., EAP-AKA' [82].

5G standardization efforts are headed towards connecting all society's elements — e.g., eHealth, intelligent transportation systems, smart buildings, industry 4.0. Thus, if critical systems are connected to 5G and an attack succeeds, the resulting impact could be catastrophic [91]. There is a broad set of 5G security challenges identified by the Next Generation Mobile Networks (NGMN) Alliance [89], [92]. Both industry and academia amply discuss a highlighted set [92], as follows: (i) flash or surge networking traffic refers specifically to massive IoT deployments; (ii) security in radio interfaces considers the medium as untrusted; (iii) user plane integrity expects placing some kind of cryptographic protection for the user data; (iv) mandatory security in the architecture as a design principle, and

not as a separate feature; (v) roaming security establishes that the user security parameters are not updated when roaming from one deployment in a different operator domain to another, this would lead to security trade-offs when implementing roaming; (vi) denial-of-Service (DoS) attacks to the infrastructure caused by exposing administrative ports in network controlling components towards the Internet; (vii) signalling storms produced by the management of orchestrated distributed systems; (viii) DoS attacks on end-devices, caused by not enforcing coping mechanisms in vendor-specific or private firmware code.

The 5G ecosystem is expected to be subject to continuous changes and modifications that will drive security improvements. Previous cellular network generations were dominated by monolithic deployments, i.e., controlled by one single administrative domain operator which maintained all the infrastructure components and services. By contrast, 5G will accommodate several specialized and modular services provided by third-party stakeholders that will provide customers with improved and tailored network services [87]. For these reasons, supporting massive scenarios present a security challenge for the signalling plane within the core network of 5G systems [91]. As an illustration, the 5G assumes that there is no trust in roaming partners. This is, that the customer home network does not trust roaming serving networks employed by the user equipment. For this reason, the 5G authentication and key agreement procedures grant total control to the customer's home network. Additionally, through these procedures, the home network can verify if the user equipment is actually connected to the legitimate roaming partner service network and not to an attacker [93].

The 5G system architecture categorizes several components in the following groups: (i) the Radio Access Network (RAN) is the last-mile infrastructure related with radio channels, such as cellular base-stations and user equipment (UE); (ii) the Core Network (5G-CN) manages mobility and roaming support, offers end-users several services, manages authentication and access control tasks, is in charge of providing the end-device a connection to the Internet, and performs accountability and billing tasks; (iii) the back-haul is the communications infrastructure that links the RAN and the 5G-CN; and (iv) non-3GPP access technologies that are integrated in the 5G system to offload using the end-user data-plan, by switching the communication channel to an auxiliary radio access technology that employs unlicensed radio bands. For example, instead of accessing the Internet through the cellular radio access network, the device may temporarily switch to WiFi. These offloading hot-spots, known as femtocells, must be directly connected to 5G RAN base-stations. An overview of the impact of Offloading in the context of 5G IoT can be found in [94].

The International Mobile Telecommunications-2020 (IMT-2020) standardization organization has defined three 5G usage scenarios [95], namely, enhanced mobile broadband (eMBB), ultra-reliable and low-latency communications (URLLC), and massive machine type communications (mMTC). The latter is the scenario corresponding to the radio requirements for massive low-power IoT use cases. In this case, the 5G standardization efforts estimate that the biggest number of attack attempts will be produced in the last-mile RAN. For this reason, authentication and key agreement in 5G are one of the major security concerns for 3GPP [91], [96]. This presumption is based on previous experience with 4G networks, where the authentication and authorization requests to the Home Subscriber Server (HSS) — the core component in charge of allowing service access to end-devices — are the main attack point.

Regarding the 5G authentication ecosystem, the trust model employed by the different methods varies depending on the EAP option employed. In 5G authentication, the following solutions are supported by default. On the one hand, 5G-AKA [97] and EAP-AKA' [82] are based on a shared symmetric key trust model. Additionally, both allow mutual authentication among the 5G network and the end-device, adopting a challenge-and-response scheme based on a common crypto-key. This means that crypto-material must be preprovided in both the end-device and the 5G core network. This crypto-material distribution is commonly done by the telco operator shipping a Universal Subscriber Identity Module (USIM) card to the end-user. While 5G-AKA and EAP-AKA' are similar, they have differences in the way that message flows take place, and how the authentication-related data is carried over within the different architecture components [97]. On the other hand, the 5G authentication also allows the use of EAP-TLS [98], which uses a public key certificate trust model. After previous real-life experiences in 4G deployments, the 5G standardization groups decided that there was a need

to improve the authentication and key agreement methods. Work in [99] presents the motivation for such improvements, as well as a comparative analysis of the authentication and key agreement features of both 4G and 5G.

Integration of Non-3GPP LPWANs in the 5G Core Network

The different access technologies commonly targeted at low-power long-range can be broadly split in two categories [87]. On the one hand, 3GPP access technologies are those defined and standardized by the 3GPP organization — e.g., Long Term Evolution for Machines (LTE-M), or NB-IoT. On the other hand, there are access technologies standardized by organizations besides the 3GPP, known as *Non-3GPP* access technologies — e.g., LoRaWAN, or Sigfox. Also, there are several other standard defining organizations involved in enabling massive IoT scenarios that have realized the relevance of 5G in several contexts of society and industry. For this reason, these organization take into consideration 5G as a building block in their own efforts [100]. For instance, the IETF considers 5G as a target framework in standardization efforts with regards to slicing, Multi-access Edge Computing (MEC), machine learning at network-level, and LPWANs. In certain occasions, they create public discussion forums, known as *Birth of Feathers* (BoF) in IETF jargon, in order to avoid the need of allocating a whole WG to relatively minor tasks. Likewise, the European Telecommunications Standards Institute (ETSI) performs standardization efforts aimed at creating building blocks that will help supporting the 3GPP and 5G ecosystem. Furthermore, some of the ETSI committee members also provide support to the technical discussions at 3GPP [100]. Similarly, the 5G Infrastructure Public Private Partnership (5G PPP) initiative funds research projects that have an impact in the 3GPP/5G standardization process. Additional organizations with 5G-related activities include: (i) the Digital Video Broadcasting (DVB) with activities related to broadcasting television over 5G, (ii) the Open Network Foundation (ONF) for activities related with software defined networks, (iii) the Multe-Fire Alliance for the use of cellular radio technologies in unlicensed radio bands, (iv) the Metro Ethernet Forum (MEF) for the standardization of system orchestration, and (v) the NGMN Alliance for the study of mobile operator requirements and giving complementary support to 3GPP standardization efforts.

In order to achieve the service requirements for 5G access networks, there are several key technology enablers [91], [101]. These enablers include ultra-densification, offloading and the use of the unlicensed radio band spectrum. Also, the security challenges of these technologies are significantly different to legacy solutions. For this reason, the access network enablers must be researched and studied from the security point of view, supporting 5G security requirements. For instance, in case of end-device burglary or fraud, the access technology must allow one authorized entity to remotely disable or re-enable the device operation mode, as to avoid further fraudulent activity coming from the stolen device [88]. Therefore, the system must protect the device's location info from passive or active attacks.

Besides the aforementioned reasons, the 3GPP also identifies the need to provide integration facilities to emerging access technologies, employing both licensed and unlicensed radio bands, being standardized by the 3GPP or by Non-3GPP organizations. This drives the need for having access to security mechanisms that enable seamless access the communication channel independent of the technology employed, during the device's lifespan [88]. This is, the integration of Non-3GPP LPWANs is a key enabler in the road-map to enabling low-power massive IoT scenarios within the 5G system. Besides, this LPWAN-5G integration must consider the security aspects related to an authenticated and authorized access to the network. To achieve this, the 3GPP has defined an architecture component for this purpose, known as Non-3GPP InterWorking Function (N3IWF) [87]. In summary, the N3IWF acts as a bridge between the Non-3GPP access technology and the 5G core network. The general consensus when integrating Non-3GPP access within the 5G system is based on supporting all technologies in a common generic way. The 5G core provides each device with a user and control data plane pair. These enable an unique interface to seamlessly communicate with the system, regardless of the access technology employed.

Fig. 3.7 shows the architecture convergence of 3GPP and non-3GPP technologies within the 5G core

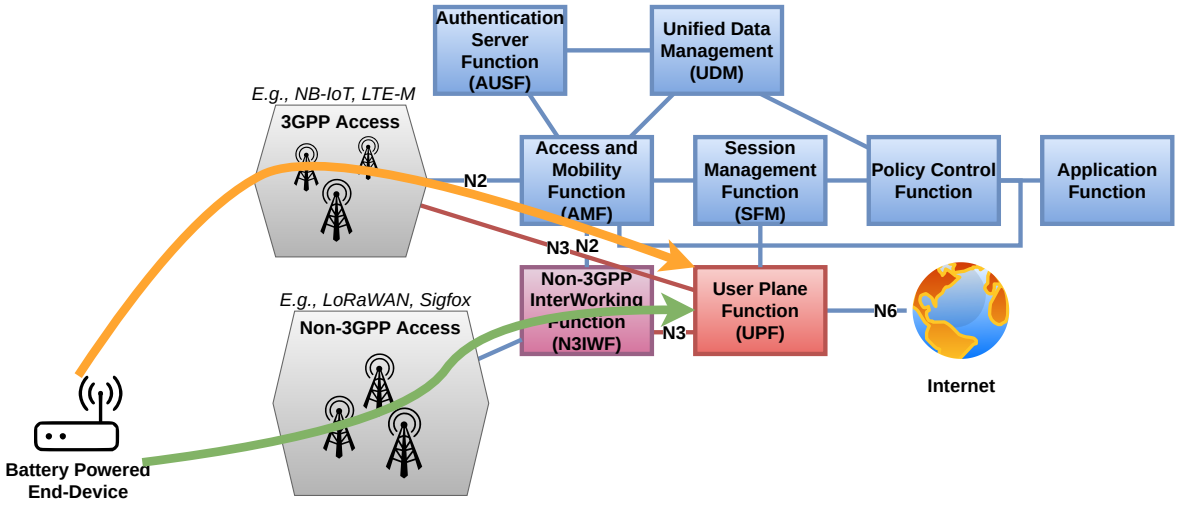

Figure 3.7: 5G architecture convergence of 3GPP and Non-3GPP access technologies.

network. As a consequence, the communication state among the end-device and the 5G core network is the same regardless of the access technology. This is, the different 5G core network components that participate in providing services to the device behave the same way regardless of the access technology being employed.

In 5G, there is only a single control plane for each connected device, it allows the 5G core to manage the UE in a seamless way. This way, the core employs the same signalling connection, address allocation, policy enforcement, data usage accountability, etc. [102]. For instance, the same Non-Access Stratum (NAS) and procedures among the UE and the 5G core are kept using the same *N1* interface. Also, the User Plane Function (UPF) employs the same Protocol Data Unit (PDU) session. As a consequence of having a common ground for the communication, the overall efficiency of the system improves because the UE may switch between 3GPP and Non-3GPP technology and only the Session Management Function (SFM) and UPF participate in the UE mobility and roaming. Having all the UE traffic anchored to the same core allows a more efficient end-to-end traffic optimization in an scalable manner. The UPF has an overall vision of all the anchored accesses — both in and out of the 5G core. At the same time, the AMF has the vision over the status of all radio link. This allows actions like load balancing, more accurate access technology selection optimization, and improving end-user throughput performance, aiming others [93].

The access of UEs to the 5G core over Non-3GPP technologies is established first by employing a signalling connection. For instance, the UE may connect to a WiFi network using confidentiality and privacy protocols outside of the 5G security scope defined by the 3GPP. Furthermore, this connection to a Non-3GPP access may not even have any kind of confidentiality or privacy protection. Hence the motivation for having a common authentication scheme for both 3GPP and non-3GPP access technologies frees the 5G core network of the specifics details of each integrated LPWAN. Regardless of the security level employed by the underlying access technology, 5G establishes its own mechanisms. The end-goal of this procedure is the creation of a secure signalling connection between the UE and serving network over un-trusted access. In order to achieve this first the UE receives an IP address from the access network that will be employed for signalling with the N3IWF. Then, the UE performs a key agreement exchange with the N3IWF using Internet Key Exchange Protocol Version 2 (IKEv2) [103]. The aim of IKE is to protect both the UE and N3IWF from possible attacks originated within the Non-3GPP access network itself — e.g., the attack over a LoRaWAN network. Later, the UE tells the N3IWF to which AMF it must connect and an IPSec [104] tunnel is created between both the UE and

the AMF. Finally, the UE exchanges NAS signalling with the 5G core to perform further 5G specific registration and authentication procedures. Finally, at this point the IKE procedure still remains in an unfinished state, known as the authentication phase. For this reason, the NAS signalling is employed to carry a 5G-specific EAP flavor [87]. As a result of this EAP exchange, the AMF provides the N3IWF with security material to complete the IKE procedure. The result of this procedure is the link shown in Fig. 3.7.

However, even if the 5G ecosystem aims a seamless Non-3GPP technology integration, there are intrinsic features found in 3GPP technologies that may not be present in other Non-3GPP LPWANs. For instance, the 5G employs a User Location Info (ULI) mechanisms to obtain the geographical location of the UE. This is achieved thanks to knowing what cellular base-station is being employed, its identifier (Cell-ID), and its location. Another feature implicit in 3GPP radio access networks is the use of extended Discontinuous Reception (eDRX), specific of technologies such as NB-IoT. This saves considerable amounts of energy by allowing battery-powered UE to stay in a sleep mode and only wake up at certain reception windows — paging periods — where the core network may need to transmit data to the UE [18], [21], [22]. Also, in 3GPP the hand-over process is defined and managed by the RAN, while in other Non-3GPP networks, it is the end-device logic which chooses how to handle cell mobility [87].

3.2.5. Gap Analysis

Research proposals aimed at supporting the continuously growing number of connected IoT devices must enable security by design, and not as an afterthought. There is a need to study and validate IoT-enabling solutions in real-life scenarios that use low-power long-range communication technologies and battery-powered hardware. These validations must take into consideration the impact of enabling IP-based architectures through different underlying networks, while also supporting security and privacy. The validated solutions must be scalable and manageable when dealing with a deployment of hundreds or thousands of heterogeneous devices within the same administrative domain. Also, in the specific case of low-power long-range communication technologies, these enablers must be validated and tested within both licensed and unlicensed radio band LPWAN technologies to cope with the different QoS limitations of each category. As a consequence, security protocols are required to be as efficient as possible in terms of bandwidth usage, power efficiency, storage, and computational power. Also, since battery-powered devices stay most of the time in sleep mode, they can only be reached by the infrastructure at certain daily time-slots. Thus, security protocols must be able to operate over delay-tolerant networks with a relatively low packet delivery rate.

Additionally, the standardization organizations in charge of cellular networks — e.g., 3GPP — have embedded the massive IoT scenarios as one of their three main key use cases for 5G core networks and deployments, namely, mMTC [95]. This implies that there are many standardization efforts headed towards supporting battery-powered constrained devices over 5G. Consequently, it is expected that these protocols will operate in both cellular network deployments that use low-power communication technologies — such as NB-IoT — in addition to vendor-specific LPWAN technologies — e.g., LoRaWAN, Sigfox.

To enable future secure IP-based deployments, these protocols must be integrable in a diverse set of bandwidth-constrained radio technologies, while traversing different vendor-specific architectures, and solutions. This must be feasible and achieved in a coherent way that will not force changes on the leveraging technologies or supporting vendor solutions. Besides, battery-powered constrained devices are expected to have a projected lifespan up to years with a 5 Ah battery [8]. During this period, the intermediate supporting infrastructures may change administrative domain, vendors, or hardware. Hence, secure protocols for IoT confidentiality or data integrity should not trust any of the underlying cellular networks or LPWANs. Regarding 5G, the current standardization efforts to integrate emerging radio access technologies do not take into consideration the exacerbating limitations of unlicensed radio conditions. Instead, they enforce authentication and authorization protocols designed without low-power technologies in mind — i.e., IPSec and IKEv2 — which are prohibitively expensive in terms

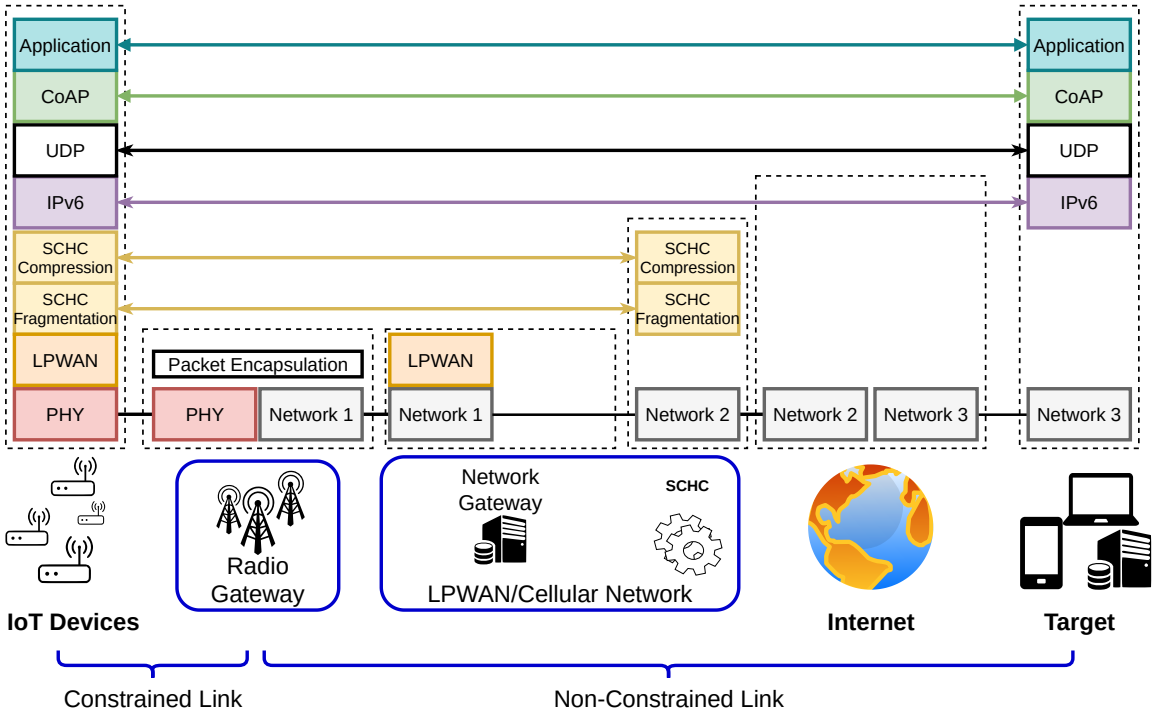

Figure 3.8: Network integration of IoT devices over low-power long-range communication technologies.

of duty-cycle and message size limitations found in LPWANs. Therefore, there is a need for solutions that enables both, the integration of Non-3GPP low-power long-range technologies in the 5G ecosystem while efficiently managing the connectivity characteristics of massive IoT end-devices through open standardized IP-based protocols.

Current related work lack a secure and scalable proposal for enabling IoT request-answer IP-based scenarios that has been implemented and validated over real-life scenarios leveraging on low-power long-range communication technologies in both cellular and vendor-specific LPWANs employing licensed and unlicensed radio technologies.

3.3. Secure Protocols in IoT Technologies Leveraging in Low-Power Long-Range Communication

The network integration of constrained IoT devices over low-power long-range communication technologies envisioned by the IETF is shown in Fig. 3.8. In order to perform an efficient transmission of IPv6/UDP/CoAP packets, the SCHC compression and fragmentation procedure, presented previously in Section 3.2.2, is employed. Thanks to the star-of-stars architecture of LPWANs [9], all the messages sent by all end-devices reach a single central network gateway. Thus, the SCHC compression and fragmentation module is integrated in the LPWAN architecture as an application server, or even be co-located with the network gateway itself. Thanks to this proposed architecture, end-devices are seamlessly integrated in the Internet, where the resources hosted into them can be addressable with an URI — e.g., `coap://2001::1/temp`.

Thanks to choosing open standardized and interoperable protocols, developers and network administrators are presented with freedom to adopt any CoAP-compatible confidentiality and privacy protection mechanisms as the *application layer* shown in Fig. 3.8. In this regard, the most promising

IETF-standardized solutions for battery-powered devices are DTLS v1.3 [55], OSCORE [54]. However, it has been shown that the massive IoT scenarios also require an efficient and scalable authentication and key exchange framework. As aforementioned in Section 3.2.3, this is achieved thanks to AAA and EAP. In this section, the solution to perform a lightweight EAP-Based secure authentication and key exchange procedure is described. This methodology leverages on header compression and low-overhead bootstrapping protocols.

3.3.1. IPv6/UDP/CoAP header compression over SCHC

As aforementioned in Section 3.2.2, the compression of IPv6/UDP can successfully compress all the header fields if the following conditions are met: (i) the network addresses of both end-points are known beforehand, and (ii) the UDP ports employed by both end-points are known — please refer to Appendix A of [15] to see compression examples that achieve this feat. Listing 3.1 shows a rule example of IPv6/UDP SCHC context C implementation. The procedure to define a SCHC context goes as follows. First, the network operator must study the different traffic flows that there will be present in the deployment. Whenever a header field value is known beforehand, that value is written in the target value (TV) context row. Next, the `EQUALS` matching operator (MO) and `NOT_SENT` compression action are added to the row. This is the most optimal solution, requiring the least computational power and bandwidth usage by omitting the transmission of this field. The rest of the possible compression actions defined in the RFC provide a worse header compression ratio. While some fields are not always known in advance, it is assumed that these are obtained by analyzing other cross-layer information. This is the case of the UDP length, which is a variable value that can be obtained by the counting the UDP payload bytes. Hence, the UDP length row can specify a `COMPUTE_LENGTH` compression action, meaning that it will not be sent over radio, but will be computed at the other end-point. Likewise, the UDP checksum includes 16 bits of integrity checking that can be computed from the complete IPv6 message.

Listing 3.1: IPv6/UDP SCHC Compression C Implementation Rule Example

```
1  /* Field;                FL; FP;DI; TV;                          MO;       CA; */
2
3  { IPV6_VERSION,          4,  1, BI, "6",                        EQUALS,  NOT_SENT           },
4  { IPV6_TRAFFIC_CLASS,    8,  1, BI, "0",                        EQUALS,  NOT_SENT           },
5  { IPV6_FLOW_LABEL,       20, 1, BI, "0",                        IGNORE,  NOT_SENT           },
6  { IPV6_PAYLOAD_LENGTH,   16, 1, BI, "0",                        IGNORE,  COMPUTE_LENGTH     },
7  { IPV6_NEXT_HEADER,      8,  1, BI, "17",                       EQUALS,  NOT_SENT           },
8  { IPV6_HOP_LIMIT,        8,  1, BI, "64",                       IGNORE,  NOT_SENT           },
9  { IPV6_DEV_PREFIX,       64, 1, BI, "FE80000000000000",         EQUALS,  NOT_SENT           },
10 { IPV6_DEVIID,           64, 1, BI, "",                         IGNORE,  DEVIID             },
11 { IPV6_APP_PREFIX,       64, 1, BI, "FE80000000000000",         EQUALS,  NOT_SENT           },
12 { IPV6_APPIID,           64, 1, BI, "0A0027FFFE542E4A",         EQUALS,  NOT_SENT           },
13
14 { UDP_DEVPORT,           16, 1, BI, "59355",                    EQUALS,  NOT_SENT           },
15 { UDP_APPPORT,           16, 1, BI, "5683",                     EQUALS,  NOT_SENT           },
16 { UDP_LENGTH,            16, 1, BI, "0",                        IGNORE,  COMPUTE_LENGTH     },
17 { UDP_CHECKSUM,          16, 1, BI, "0",                        IGNORE,  COMPUTE_CHECKSUM   },
```

The compression of CoAP headers using SCHC as a generic framework was recently standardized by the IETF as RFC8824 [67]. There are a set of considerations to take into account when applying SCHC to CoAP. As opposed to IPv6 and UDP, CoAP has a variable number of fields embedded within the header, known as *CoAP options* [25]. Also, the CoAP header format is asymmetric, where CoAP requests may have a different structure to their corresponding answers. Additionally, the URI path is mandatory in the request but does not appear in the response. A request may contain an *Option Accept*, while the corresponding response may contain a *Content Option*. This illustrates the asymmetric nature of CoAP. Moreover, in a CoAP exchange, both end-points may act as client, server,

Figure 3.9: EAP architecture components.

or both. But, if one end-point is always expected to act as one or the other, this can be exploited to further compress the headers.

3.3.2. SCHC Header Compression for EAP-Based Secure Authentication

EAP-Based Authentication Service over CoAP (CoAP-EAP) [105] is an EAP based lightweight authenticated key agreement mechanism, which currently is an IETF ACE WG item [106]. It leverages on CoAP as an application layer in order to exchange messages over a broad spectrum of low-power long-range technologies. As aforementioned in Section 3.2.1, the IETF estimates that future massive IoT scenarios over low-power networks will integrate CoAP as request-answer application layer protocol. For this reason, by leveraging on CoAP for the authenticated key agreement process, the overall deployment architecture is more cohesive and relies on a smaller set of technologies, reducing both the managerial complexity and end-device's firmware binary code.

CoAP-EAP allows an end-device to obtain a session key that can be employed for further communication exchanges in a secure and authenticated way. In EAP-Based protocols, the crypto material is not transmitted over the radio channel, instead it is obtained locally by both parties from other data units exchanged, e.g., nonces or identifiers.

On top of that, there is another research proposal that further builds on CoAP-EAP advancements, namely, Low-Overhead CoAP-EAP (LO-CoAP-EAP) [32]. It is more constrained in contrast with the CoAP-EAP presented in [105] by reducing the number of messages needed in the exchange and the overall size of the messages themselves. For more details on the advancements of LO-CoAP-EAP over CoAP-EAP, please refer to section 4.6 of [32]. The performance of LO-CoAP-EAP over a real-life NB-IoT scenario has been studied in [121]. The authors conclude that it is a feasible solution for performing authentication and key agreement by constrained devices in a cellular low-power long-range technology. For these reasons, we consider the use of LO-CoAP-EAP as an EAP-based lightweight authentication and key agreement platform.

CoAP-EAP follows the same architecture and data flow of the standard EAP [34]. The CoAP-EAP architecture is composed by three different parties as shown in Fig. 3.9. First, the EAP Peer is the entity attempting to access the network through an edge element, such as a radio gateway or access point. EAP does not make a distinction between the end-device and the end-customer when the term *peer* is employed, however within the context of massive IoT scenarios it is reasonably to think that one single end-user may own and manage several devices, henceforth referred as *peers* in this discussion. Secondly, the EAP authenticator is the edge component in charge of enforcing the authorized access to a network or resources. Lastly, the authentication server, also known as EAP server, is the central end-point of the authentication and key agreement phase. Please note that the EAP standard [34] also supports a two-party architecture where both the authenticator and authentication server are co-located in one single component, ending the authentication procedure there. Regardless, we focus on the typical three-party scenario where each component is differentiated.

EAP has four different message types, namely, request, response, success, and failure. The overall authentication procedure is shown in Fig. 3.10 and goes as follows: First, the peer will send to the authenticator a request leveraging in an underlying lightweith protocol stack, such as the case of LO-CoAP-EAP. This first message in step 1 is sent using the CoAP No-Response option [107] as a way to indicate that the peer does not expect an answer to this request. Next, the authenticator relies

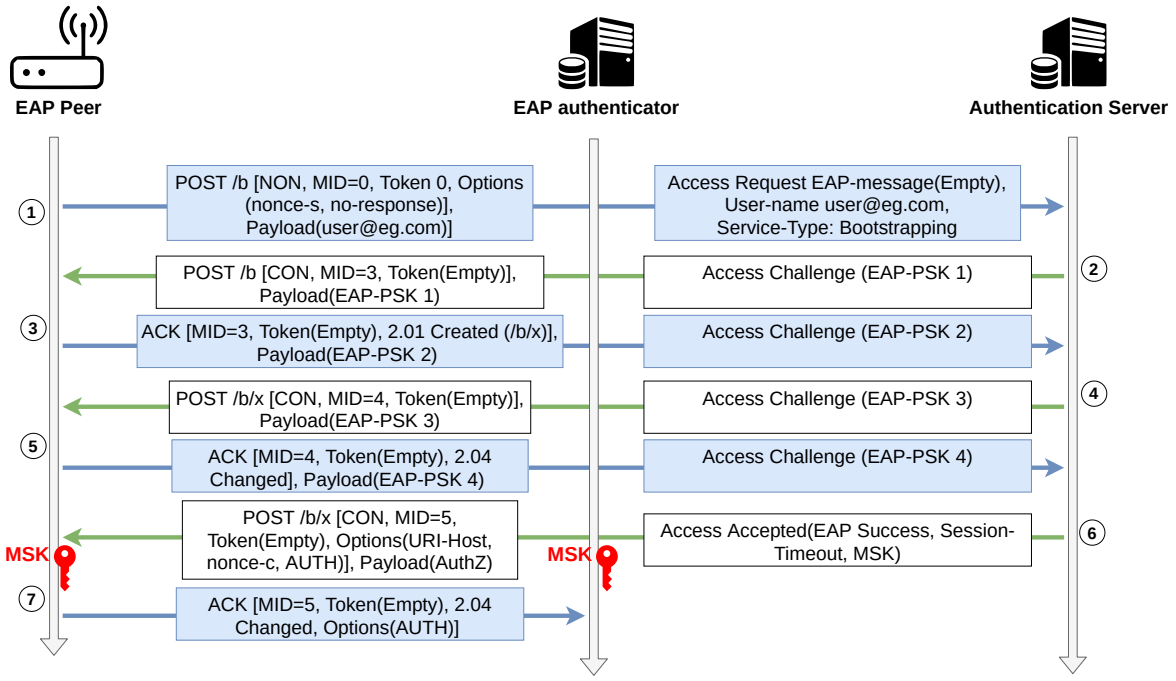

Figure 3.10: LO-CoAP-EAP dataflow exchange using EAP-PSK as an EAP Method.

the message to the authentication server using some form of standard AAA protocol, such as Remote Authentication Dial In User Service (RADIUS) [108] or Diameter [109]. Later, the authentication server receives the EAP request and verifies which policies and EAP methods apply to the end-device. Thus, the authentication server starts a series of challenge message exchanges towards the end-device in order to guarantee an authenticated and secure key agreement procedure. These request-response messages are carried over the authenticator, which will employ the end-device preferred EAP method available, e.g., LO-CoAP-EAP. Also, during this EAP challenge request-response exchange, the peer will play the role of CoAP server instead of client. This is because this way the firmware logic in the device is simplified thanks to not implementing timeouts or retransmission logic. Hence, during the challenge the authenticator plays the role of CoAP client. Lastly, the attempting end-device will either receive an EAP Success or EAP Failure message, depending on the outcome of the exchange.

As aforementioned, LO-CoAP-EAP is designed to allow a full EAP exchange while reducing the number of flights and their message lengths. In order to provide access to a wide spectrum of heterogeneous battery-powered devices, LO-CoAP-EAP allows the use of several EAP methods, whoever, to further reduce these exchanges the pre-shared key EAP method (EAP-PSK) [110] has been chosen.

After step 6 in the LO-CoAP-EAP procedure, both the end-device and authenticator share a copy of the Master Session Key (MSK). From this point onward, the authentication server does not participate in further user-data exchanges and the architecture relies solely on the peer and the authenticator. For this reason, both are required authenticate themselves mutually. In order to achieve this trust relationship, step 7 does not require the authentication server's participation and is considered outside of the EAP challenge scope. In this step, both participating parties hold a copy of the MSK and all the previous exchanged messages during steps 1–6. Next, both obtain a Transient Session Key (TSK) [34] by performing a One-key Message Authentication Checksum (OMAC) locally as shown in Equation 3.1.

$$Transient\_Session\_Key = OMAC(MSK, Sequence\_of\_messages\_exchanged) \tag{3.1}$$

Please note that the TSK is never transmitted over the radio channel. The motivation to employ the TSK instead of the MSK in this procedure is that the MSK may be shared among different entities, however, the only other entity that has a copy of both the MSK and a copy of all the exchanged packets in steps 1–6 is the participating authenticator. That is the entity in particular that the peer aims to authenticate. Besides, the TSK may be obtained by the negotiated cyphersuite shared by both entities because the authentication server does not participate in the following exchanges. Finally, both parties can prove that they own a copy of the TSK without extra messages. They both realize a 16-byte hash of the last transmitted message in step 6. The authenticator creates the PDU of step 6 and zeroes the 16-byte hash. Next, it computes its OMAC using the TSK as shown in Equation 3.2. The obtained result gets stored in the corresponding 16-byte MAC field and sent over to the peer. In turn, the peer does the exact same procedure. If the MAC received in the message and the one calculated locally match, the peer infers that the authenticator owns the TSK. Next, in step 7 the peer sends the CoAP ACK also with a 16-byte MAC field using the same procedure employed in step 6 (Equation 3.2). When the authenticator receives the step 7 message, it authenticates the peer.

$$Step\_6\_message\_MAC = OMAC(TSK, Step\_6\_message\_with\_zeroed\_MAC) \tag{3.2}$$

In order to support the aforementioned mutual authentication procedure, LO-CoAP-EAP extends the CoAP protocol with a custom CoAP Option field in with identifier 92. This custom field always contains a 16-byte hash MAC with random data. It is referred by LO-CoAP-EAP as `COAP_OPTION_AUTH`. Please note that keys are never transmitted over radio during this mutual authentication procedure.

Once the LO-CoAP-EAP message field and characteristics have been established, there is enough understanding for a network administrator to define the static context rules that can achieve high compression ratios. Listing 3.2 shows a LO-CoAP-EAP compression rule example, specifically it is applied for the step 1 of Fig. 3.10. First, as can be seen in the example, all the rule rows from `COAP_VERSION` to `COAP_CODE` employ the `NOT_SENT` SCHC compression action and are not transmitted over the radio channel. This is thanks to knowing beforehand that this message is a CoAP `NON` packet with a code `0.02 POST`. Also, there will be only one single LO-CoAP-EAP authentication procedure running at each moment in time, thus the CoAP token feature is not required, i.e., all these messages have an empty token with a TKL value of 0. Next, the `COAP_MESSAGE_ID` is sent over the constrained radio link due to it being random [25]. Please note that Fig. 3.10 shows MID values 0–5 for clarity, but in fact these can be totally random. Later, the headers can include several CoAP options, each with a variable length iself. For these reasons, the CoAP employs a simple serialization format where the option content type and its length must be provided before the option payload itself. Following this logic, based on the specification of LO-CoAP-EAP we can establish that the resource path — CoAP URI path — will always be `/b`, hence we do not need to send that value over the network either. Then, the second CoAP option includes a 4-byte nonce that cannot be predicted and is sent over the radio channel. Finally, the last CoAP option in this example is employed for a No-Response option [107].

Listing 3.2: LO-CoAP-EAP SCHC Compression C Implementation Rule Example

```
/* Field;                FL; FP;DI; TV;       MO;       CA; */

/* ... */

{ COAP_VERSION,          2,  1, BI, "1",      EQUALS,  NOT_SENT   },
{ COAP_TYPE,             2,  1, BI, "1",      EQUALS,  NOT_SENT   },
{ COAP_TKL,              4,  1, BI, "0",      EQUALS,  NOT_SENT   },
{ COAP_CODE,             8,  1, BI, "2",      EQUALS,  NOT_SENT   },
{ COAP_MESSAGE_ID,       16, 1, BI, "0",      IGNORE,  VALUE_SENT },
{ COAP_TOKEN,            16, 1, BI, "0",      IGNORE,  NOT_SENT   },
{ COAP_OPTION_DELTA,     4,  1, BI, "11",     EQUALS,  NOT_SENT   },
{ COAP_OPTION_LENGTH,    4,  1, BI, "1",      EQUALS,  NOT_SENT   },
{ COAP_OPTION_VALUE,     8,  1, BI, "b",      EQUALS,  NOT_SENT   },
{ COAP_OPTION_DELTA,     4,  2, BI, "28",     EQUALS,  NOT_SENT   },
{ COAP_OPTION_LENGTH,    4,  2, BI, "4",      EQUALS,  NOT_SENT   },
{ COAP_OPTION_VALUE,     32, 2, BI, "",       IGNORE,  VALUE_SENT },
{ COAP_OPTION_DELTA,     4,  3, BI, "29",     EQUALS,  NOT_SENT   },
{ COAP_OPTION_LENGTH,    4,  3, BI, "1",      EQUALS,  NOT_SENT   },
{ COAP_OPTION_VALUE,     8 , 3, BI, "",       IGNORE,  VALUE_SENT },
```

Once all the CoAP header fields have been processed, the compressor finds the CoAP option ending mark, which is a `0xFF` octet. The remaining bytes of the message include the payload. This payload is not compressed by the SCHC CoAP compression mechanism as it is mostly unpredictable due to the EAP challenge carrying nonces, hashes and MAC fields when performing LO-CoAP-EAP. The rest of the messages depicted in 3.10 have their own SCHC context rule, relatively similar to the one shown in 3.2. Thanks to using EAP-PSK as an EAP method, LO-CoAP-EAP exchanges cryptographic material of relatively predictable lengths, improving the compression ratio. However, due to the randomness of nonces, hashes and other cryptograhpic related material, the current context rules do not provide a comprehensive and generic solution to predict those. This is also the case of data carried as CoAP payload, which is elided by the SCHC compression mechanism altogether in its current state.

3.3.3. NB-IoT Real-Life Evaluation and Validation

Validation experiments were performed with real-life hardware in order to validate the research proposal presented in Section 3.3 over two of the most popular LPWAN technologies identified by the IETF in [9], namely, NB-IoT and LoRaWAN. First, LO-CoAP-EAP was evaluated as an EAP-based authentication and key agreement protocol in contrast with the Protocol for Carrying Authentication for Network Access (PANA) [31], [111]. This evaluation was performed over real-life hardware in an NB-IoT deployment and analyzed the number of messages exchanged, their size, and the average total time to perform the authentication procedure. As opposed to LO-CoAP-EAP, PANA does not employ CoAP, which provides features related to reliability and re-transmission mechanisms. In turn, PANA leverages on UDP and requires to implement its own reliability and re-transmission mechanisms. The results of this evaluation are shown in Table 3.1 and Fig. 3.11. Both protocols employed the same EAP method, i.e., EAP-PSK, thus both PANA and LO-CoAP-EAP carried the same underlying cryptographic information. Additionally, Table 3.1 showcases the NB-IoT PDU size, which includes all the underlying network layers' overhead.

During these tests, NB-IoT was employed as the LPWAN technology at the radio physical layer, nevertheless, in order to connect the end-device to the Internet through a cellular network, it transmits the headers of all the IP-based network stack, i.e., all the bytes related to the cellular MAC, IP and UDP headers were transmitted over the constrained radio link. This feat is possible thanks to cellular networks employing a licensed radio band, which provides a significantly higher minimum

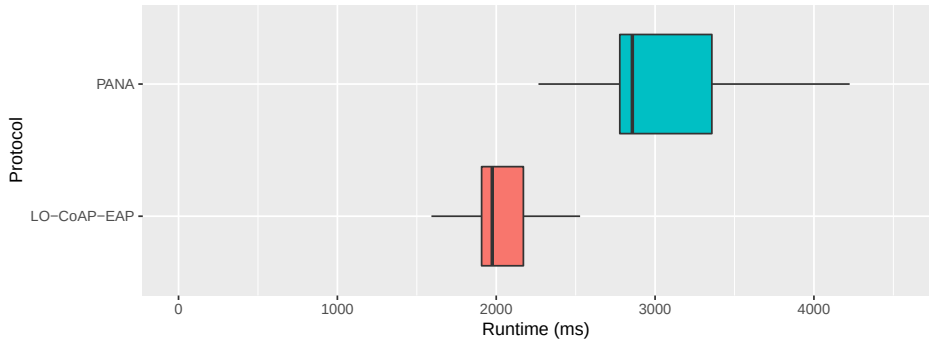

Figure 3.11: Authentication total run-time distribution over NB-IoT. Extracted from [121].

QoS than their unlicensed-radio band counterparts. However, since the battery lifespan of constrained end-devices is a key performance factor when evaluating LPWANs, transmitting all the IP-related headers uncompressed over the network is not considered as efficient. To extend the reach of these results, the performance of LO-CoAP-EAP was also validated over LoRaWAN using the SCHC header compression and fragmentation mechanism while enabling the integration with the Internet.

Table 3.1: Length of messages exchanged in LO-CoAP-EAP and PANA. Extracted from [121].

Protocol	Message	Message Length	NB-IoT PDU Length
LO-CoAP-EAP	POST	29	67
	POST(EAP-PSK1)	36	74
	ACK(EAP-PSK2)	69	107
	POST(EAP-PSK3)	68	106
	ACK(EAP-PSK4)	48	86
	POST(EAP-Success)	38	76
	ACK	23	61
	Total	**311**	**577**
PANA	PCI	16	54
	PAR	40	78
	PAN	40	78
	PARReq(Id)	48	86
	PANRep(Id)	60	98
	PAR(EAP-PSK1)	56	94
	PAN(EAP-PSK2)	84	122
	PAR(EAP-PSK3)	84	122
	PAN(EAP-PSK4)	68	106
	PAR(EAP-Success)	88	126
	PAN	52	90
	Total	**636**	**1054**

3.3.4. LoRaWAN Real-Life Evaluation and Validation

LoRaWAN [17], [112], [113] is an LPWAN technology supported by the LoRa Alliance [19], a consortium formed by companies such as Cisco or Semtech. It employs an open-specification MAC

[19] https://lora-alliance.org/

layer [112] on top of a long-range LoRa physical layer [114] based on the Chirp Spread Spectrum (CSS) radio modulation. LoRaWAN is designed with battery-powered constrained devices in mind, aiming to reduce the cost per device when facing massive deployments. LoRaWAN has gained attention from both industry and academia due to its capacity for serving up to thousands of devices per cell, while providing a coverage range up to tens of kilometers [14], [65], [115], [116].

In order to validate the proposed solution above over an LPWAN technology constrained to the regulations of an unlicensed radio band technology, a real-life LoRaWAN deployment scenario was employed to evaluate the use of LO-CoAP-EAP. The results of this validation can be found in [127], where a combination of the SCHC and LO-CoAP-EAP ran on embedded hardware, while circulating on board a vehicle, performing the authenticated key agreement procedure. In order to support the different LoRaWAN data-rate modes, the different compressed packets went through a fragmentation procedure in order to fit in the LoRaWAN maximum application payload size of 51 bytes for the longest coverage range mode on ISM 868 MHz radio band [41], [113]. Table 3.2 shows the resulting LO-CoAP-EAP message compression ratios, extracted from [127]. Thanks to the SCHC header compression mechanisms, five out of seven packets fit within a single LoRaWAN message in its longer coverage-range configuration. The rest were fragmented in two different fragments of 40 payload bytes each, enabling their transmission over the network.

Table 3.2: IPv6 and SCHC packet size and compression ratios. Extracted from [127]

LO-CoAP-EAP	Direction	IPv6 Payload (B)	SCHC Packet no fragmentation (B)	CoAP Payload (B)	SCHC Compression Ratio (%)
Message 1	Uplink	85	16	8	18.8
Message 2	Downlink	98	32	29	32.6
Message 3	Uplink	131	66	60	50.3
Message 4	Downlink	130	65	59	50.0
Message 5	Uplink	110	48	43	43.6
Message 6	Downlink	100	28	4	28.0
Message 7	Uplink	85	19	0	22.3

3.4. Lessons Learned and Conclusions

As previously happened with the Internet, now the IoT paradigm is part of our lives. It has come to stay, presenting innovative and unprecedented solutions to complex problems found in productive fabrics. The predictions estimate a continuous growth in the market value and number of devices connected, for years to come. This fosters heterogeneous and massive scenarios where several vendors compete. Among the different applications of the IoT paradigm, one of the prominent ones revolves around remote control and monitoring solutions, with cost-effective sensor and actuator devices scattered in sparse geographical locations, typically working under harsh or adverse climate conditions. Besides, these devices are meant to be deployed and operate without human supervision, even lacking keypads or displays. This is a design choice that not only focuses in reducing per-device cost, but also out of pure necessity, since some of these devices are unreachable — e.g., devices installed under a layer of asphalt or in hard-to-reach locations. Additionally, in these scenarios there is no power-grid available for end-devices, and many times, there is no regular cellular coverage, i.e., do not presume having 4G/5G reception. These applications commonly include, but are not limited to Smart Cities, Industry 4.0, and Smart Agriculture. As a consequence, different vendors are driven into presenting novel market-ready products and services.

Remote monitoring and control solutions found in the aforementioned applications, usually revolve around extending the reach of sensor and actuator end-devices. The more end-devices deployed further, the better. For this reason, there is a focus on reducing the cost per end-device. To achieve this, domain administrators are focusing their efforts on developing embedded hardware solutions, based in low-cost and power-efficient microcontroller solutions — also known as system-on-chips (SoC) and more specifically referred to as constrained devices by the IETF. These are devices that have very limited

computational and storage capacities, that run a relatively simple operation logic, which is unlikely to change over the end-device life-cycle. Aligned with this idea, the aforementioned applications consider a lack of power-grid available in the target device location, thus focusing on devices powered by batteries.

In order to solve the aforementioned power and connectivity challenges of these scenarios, one of the solutions have partially filled this gap are Low-Power Wide Area Networks (LPWANs). These are infrastructures that provide affordable connectivity to large coverage areas, targeting constrained devices, through long-range low-power physical radio modulations techniques. End-devices save battery-power by running most of the time on a low-power mode — known as *sleep* — periodically entering the regular full-power mode to transmit small packets over radio. As a consequence, the adopted LPWAN technology employed has a large impact in what kind of scenarios the infrastructure can support and their overall architecture and components.

Different vendors rushed to launch market-ready LPWAN solutions, understandably so, since there was a large market share to be taken. For this reason, companies entered a race against the clock, which led to taking chances with their designs and commercial approaches, making questionable decisions that have been discussed and explored by both industry and academia. Each LPWAN technology approached the solution with different intentions and goals. Sigfox tries to offer an all-in-one solution, taking away from the customer as many underlying technical details as possible, charging end-users a monthly subscription fee for each one of their connected devices. Then, Sigfox provides the operation and maintenance of a private and closed radio back-haul network and central operation platform, facilitating an interface for the customer application servers while hiding all the details.

Another relevant alternative is LoRaWAN, a polar-opposite approach to LPWANs. In LoRaWAN, the specification is open and accessible to the general public. There is no licensing, so anyone can implement and deploy any of the LoRaWAN architecture components totally free of charge. This approach enables a service-based business model, where many different companies may offer their LoRaWAN infrastructure components for a fee, and lets end-customers to choose if they prefer to either implement the supporting components themselves, or hire a third-party instead. The drawback of this open and modular approach is that end-customers are forced to survey the myriad of LoRaWAN-based market-ready services and solutions that best fit their application.

In addition, the 3GPP created NB-IoT and LTE-M as cellular-based LPWAN solutions. These were designed from the start with one major goal in mind, namely, to run on already existing 4G/LTE cellular deployments. The idea was to enable them by simply performing a software update on the cellular radio access infrastructure, i.e., the cellular base-stations and the LTE core. Thus, employing pre-existing radio modulation schemes and the same LTE core internal protocols. This gives both NB-IoT and LTE-M a huge head-start, thanks to leveraging on a globally available 4G cellular coverage. However, this backwards-compatibility strategy led to some arguably design choices that may hinder its success. For instance, the necessity on relying on your local telco service providers to update their infrastructure for NB-IoT/LTE-M support, without giving any control over this to the customer. Besides, most, if not all, NB-IoT/LTE-M current market ready products are based on the cellular service subscription strategy, where the end-user pays a monthly fee per device, severely increasing the cost-per-device. While some NB-IoT chips are able to employ unlicensed radio bands, in practicality, it is not a service commonly provided by cellular telcos, due to their lack of interest in such matter. Therefore, as can be seen, the LPWAN chosen is a careful decision that mast be taken during the planning and design stage of every large-scale project, potentially risking the failure of the end-product.

Regarding security in LPWANs, as what happens in today's common Internet web-based interactions, end-users do not trust their service providers to enforce the confidentiality and privacy of their data. This has spawn a variety of end-to-end trust and confidentiality solutions over common IP-based protocols and frameworks. Due to the IoT-LPWAN popularity, these basic security principles are currently being translated to the constrained environment. As a result, numerous standardization efforts by different SDOs focus on enabling trust in constrained hardware and low-bandwidth networks. Since each LPWAN technology uses tailor-specific security mechanisms, each deployment lacks interoperability with third-party data networks, connected through the Internet, generating connectivity isolated islands that present a problem for domain administrators relying in heterogeneous IoT solutions.

During this PhD thesis research period, the main goal has been to design, implement, and validate novel secure protocols for the IoT paradigm over long-range low-power technologies. The feasibility and requirements for transmitting information over constrained channels were studied within the context of embedded hardware in a secure manner. For this, different research proposals were surveyed for the secure bootstrapping and integration of LPWANs with the Internet, as well as in 5G systems over embedded hardware. The results indicate that common Internet protocols employed in commodity hardware are not apt for constrained environment due to their stringent power and connectivity requirements. Additionally, the integration of third-party non-3GPP LPWAN technologies within the 5G ecosystem requires novel secure lightweight authentication and key agreement solutions that further improve on the solutions proposed.

As aforementioned, the number of connected IoT devices is expected to grow at a steady pace in coming years. This will drive the depletion of the current IPv4 address space, forcing these devices to employ IPv6 addressing instead. However, IPv6 packets contain a mandatory 40-byte length header, combined with an MTU of 1280 bytes. Considering that LPWAN technologies are designed to transmit packets in the order of 10's of bytes, a fixed 40-byte header is prohibitively expensive. Also, LPWANs are message-oriented communication technologies, so stream-based protocols are not expected or directly supported by vendors. For this reason, current LPWANs require a fragmentation and reassembly mechanism. In order to support the seamless integration of different LPWAN devices with the Internet, a header compression and fragmentation mechanism for the transmission of IPv6/UDP/CoAP packets was implemented and validated over real-life embedded hardware, connected through a LoRaWAN deployment. The results indicate that the Static Context Header Compression (SCHC) mechanism proposed by the IETF LPWAN WG presents a valid solution for the integration of devices within the Internet, while saving both radio bandwidth and battery power.

Due to the diverse LPWAN market, each vendor has rushed to provide basic security mechanisms that enforce a certain level of over-the-air confidentiality and privacy. However, these solutions are not interoperable, and, in some instances not even provide the technical specification details publicly. For this reason, the integration of LPWANs within the Internet requires the use of openly standardized solutions that enable these devices to run on this hardware. To address the aforementioned challenges, a lightweight secure and authentication key agreement technique for constrained environments, namely, LO-CoAP-EAP, was implemented and validated over a real-life NB-IoT deployment. The results indicate that the LO-CoAP-EAP bootstrapping mechanism is a valid solution to provide an scalable and human-centric technique in LPWANs.

Lastly, an efficient lightweight secure authentication and key agreement LO-CoAP-EAP scenario was implemented and evaluated over a real-life LoRaWAN deployment, leveraging on the seamless IPv6 integration through the SCHC mechanisms for mobile scenarios. The results demonstrate that the proposed solution provides LoRaWAN devices the capability to directly interact with domain-controlled authentication servers accessible through the Internet.

Future ways for this research include the further seamless integration of new kinds of constrained devices within the Internet. We would like to highlight that during the PhD research period, the Satellite Communications Department at the European Space Agency (ESA) has shown interest in the research results related to the header compression and fragmentation of IP-based protocols for LoRaWAN networks. Their aim is to exploit the solution implemented in this thesis in the context of low orbit satellital communications, in order to provide remote end-devices with IPv6 connectivity towards the Internet. After contacting us, it is expected in the foreseeable future to perform integration and evaluation tests using the validated implementation. In this line of work, it is expected to further improve the reach and capabilities of SCHC for security-related lightweight authentication and key agreement protocols, as well as application level security mechanisms. These efforts are aimed at compressing the headers of both Object Security for Constrained RESTful Environments (OSCORE) and Ephemeral Diffie-Hellman Over COSE (EDHOC).

One framework that would clearly benefit from these header compression contributions would be the Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth) [35]. This is an standardization effort that aims at support OAuth

2.0 over constrained environments, leveraging on OSCORE and EDHOC. Also, to further improve the bootstrapping procedure, novel Machine Learning (ML) techniques may be employed to create statistical models that would offer better performance over the aforementioned scenarios, such as TinyML [117], [118].

CHAPTER 4

Publications Composing the PhD Thesis

4.1. Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions

Title	Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions
Authors	Jesus Sanchez-Gomez and Dan Garcia-Carrillo and Ramon Sanchez-Iborra Jose Luis Hernandez Ramos and Jorge Granjal and Rafael Marin-Perez and Miguel Angel Zamora Izquierdo
Type	Journal
Journal	IEEE Access
Impact factor (2020)	3.367
Publisher	IEEE
Pages	216437 - 216460
Volume	8
Year	2020
Month	November
ISSN	2169-3536
DOI	http://dx.doi.org/10.1109/ACCESS.2020.3041057
URL	https://ieeexplore.ieee.org/document/9272765/
State	Published
Author's contribution	The PhD student, Jesus Sanchez-Gomez, is the main author of the paper

Journal details: IEEE Access
ISSN: 2169-3536
Publisher: IEEE
Impact factor (2020): 3.367
Website: `https://ieeeaccess.ieee.org/`

Authors – Personal details	
Name	**Jesús Sánchez Gómez**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia (Spain)
Name	**Dr. Dan García Carrillo**
Position	Assistant Professor in the Computer Science Department
University	University of Oviedo (Spain)
Name	**Dr. Ramon Jesús Sánchez Iborra**
Position	Assistant Professor
University	University Center of Defense, San Javier Air Force Base (Spain)
Name	**Dr. José Luis Hernández Ramos**
Position	Postdoctoral Researcher
Research Centre	European Commission Joint Research Centre in Ispra (Italy)
Name	**Dr. Jorge Granjal**
Position	Assistant Professor (Informatics Engineering)
University	University of Coimbra (Portugal)
Name	**Dr. Rafael Marín Pérez**
Position	Postdoctoral researcher
Company	Odin Solutions S.L. (Spain)
Name	**Dr. Miguel Ángel Zamora Izquierdo**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia (Spain)

Abstract

The convergence of the Internet of Things (IoT) and 5G will open a range of opportunities for the deployment of enhanced sensing, actuating and interactive systems as well as the development of novel services and applications in a plethora of fields. Given the processing and communication limitations of both IoT devices and the most novel IoT transmission technologies, namely, Low Power Wide Area Network (LPWAN), there are notable concerns regarding certain security issues to be overcome in order to achieve a successful integration of LPWAN systems within 5G architectures. In this survey work, we analyze the main security characteristics of LPWANs, specially focusing on network access, and contrast them with 5G security requirements and procedures. Besides, we present a comprehensive review and analysis of research works proposing security solutions for the 5G-LPWAN integration. Finally, we explore open issues and challenges in the field and draw future research directions. From our analysis, it is evident that many efforts are being devoted from the academia, industry and Standards Developing Organizations (SDOs) for achieving the desired confluence of IoT and 5G worlds. We envision a successful integration of both ecosystems by exploiting novel lightweight security schemes addressing the stringent security requirements of 5G while being assumable by constrained IoT devices.

4.2. Impact of SCHC Compression and Fragmentation in LPWAN: A Case Study with LoRaWAN

Title	Impact of SCHC Compression and Fragmentation in LPWAN: A Case Study with LoRaWAN
Authors	Jesus Sanchez-Gomez and Jorge Gallego-Madrid and Ramon Sanchez-Iborra and Jose Santa and Antonio F. Skarmeta Gómez
Type	Journal
Journal	Sensors
Impact factor (2020)	3.576
Publisher	MDPI
Article Number	280
Volume	20
Issue	1
Year	2020
Month	January
ISSN	1424-8220
DOI	https://doi.org/10.3390/s20010280
URL	https://www.mdpi.com/1424-8220/20/1/280
State	Published
Author's contribution	The PhD student, Jesus Sanchez-Gomez, is the main author of the paper

Journal details: Sensors
ISSN: 1424-8220
Publisher: MDPI
Impact factor (2020): 3.576
Website: `https://www.mdpi.com/journal/sensors`

Authors – Personal details	
Name	**Jesús Sánchez Gómez**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia (Spain)
Name	**Jorge Gallego Madrid**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia (Spain)
Name	**Dr. Ramon Jesús Sánchez Iborra**
Position	Assistant Professor
University	University Center of Defense, San Javier Air Force Base (Spain)
Name	**Dr. José Santa Lozano**
Position	Postdoctoral Researcher
University	Technical University of Cartagena (Spain)
Name	**Dr. Antonio F. Skarmeta Gómez**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia (Spain)

Abstract

The dawn of the Internet of Things (IoT) paradigm has brought about a series of novel services never imagined until recently. However, certain deployments such as those employing Low-Power Wide-Area Network (LPWAN)-based technologies may present severe network restrictions in terms of throughput and supported packet length. This situation prompts the isolation of LPWAN systems on islands with limited interoperability with the Internet. For that reason, the IETF's LPWAN working group has proposed a Static Context Header Compression (SCHC) scheme that permits compression and fragmentation of and IPv6/UDP/CoAP packets with the aim of making them suitable for transmission over the restricted links of LPWANs. Given the impact that such a solution can have in many IoT scenarios, this paper addresses its real evaluation in terms not only of latency and delivery ratio improvements, as a consequence of different compression and fragmentation levels, but also of the overhead in end node resources and useful payload sent per fragment. This has been carried out with the implementation of middleware and using a real testbed implementation of a LoRaWAN-to-IPv6 architecture together with a publish/subscribe broker for CoAP. The attained results show the advantages of SCHC, and sustain discussion regarding the impact of different SCHC and LoRaWAN configurations on the performance. It is highlighted that necessary end node resources are low as compared to the benefit of delivering long IPv6 packets over the LPWAN links. In turn, fragmentation can impose a lack of efficiency in terms of data and energy and, hence, a cross-layer solution is needed in order to obtain the best throughput of the network.

4.3. Secure Authentication and Credential Establishment in Narrowband IoT and 5G

Title	Secure Authentication and Credential Establishment in Narrowband IoT and 5G
Authors	Jesus Sanchez-Gomez and Dan Garcia-Carrillo and Rafael Marin-Perez and Antonio F. Skarmeta Gómez
Type	Journal
Journal	Sensors
Impact factor (2020)	3.576
Publisher	MDPI
Article Number	882
Volume	20
Issue	3
Year	2020
Month	February
ISSN	1424-8220
DOI	https://doi.org/10.3390/s20030882
URL	https://www.mdpi.com/1424-8220/20/3/882
State	Published
Author's contribution	The PhD student, Jesus Sanchez-Gomez, is the main author of the paper

Journal details: Sensors
ISSN: 1424-8220
Publisher: MDPI
Impact factor (2020): 3.576
Website: `https://www.mdpi.com/journal/sensors`

Authors – Personal details	
Name	**Jesús Sánchez Gómez**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia (Spain)
Name	**Dr. Dan García Carrillo**
Position	Assistant Professor in the Computer Science Department
University	University of Oviedo (Spain)
Name	**Dr. Rafael Marín Pérez**
Position	Postdoctoral researcher
Company	Odin Solutions S.L. (Spain)
Name	**Dr. Antonio F. Skarmeta Gómez**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia (Spain)

Abstract

Security is critical in the deployment and maintenance of novel IoT and 5G networks. The process of bootstrapping is required to establish a secure data exchange between IoT devices and data-driven platforms. It entails, among other steps, authentication, authorization, and credential management. Nevertheless, there are few efforts dedicated to providing service access authentication in the area of constrained IoT devices connected to recent wireless networks such as narrowband IoT (NB-IoT) and 5G. Therefore, this paper presents the adaptation of bootstrapping protocols to be compliant with the 3GPP specifications in order to enable the 5G feature of secondary authentication for constrained IoT devices. To allow the secondary authentication and key establishment in NB-IoT and 4G/5G environments, we have adapted two Extensible Authentication Protocol (EAP) lower layers, i.e., PANATIKI and LO-CoAP-EAP. In fact, this approach presents the evaluation of both aforementioned EAP lower layers, showing the contrast between a current EAP lower layer standard, i.e., PANA, and one specifically designed with the constraints of IoT, thus providing high flexibility and scalability in the bootstrapping process in 5G networks. The proposed solution is evaluated to prove its efficiency and feasibility, being one of the first efforts to support secure service authentication and key establishment for constrained IoT devices in 5G environments.

CHAPTER 5

References

[1] K. Ashton and Others, "That 'internet of things' thing", *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013, ISSN: 0167739X. DOI: 10.1016/j.future.2013.01.010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X13000241https://linkinghub.elsevier.com/retrieve/pii/S0167739X13000241.

[3] A Ericsson, "Cellular networks for massive iot—enabling low power wide area applications", *no. January*, pp. 1–13, 2016.

[4] S. Lucero and Others, "IoT platforms: enabling the Internet of Things", *White paper*, 2016.

[5] N. Heuveldop and Others, "Ericsson Mobility Report; Ericsson AB, Technol. Emerg. Business, Stockholm", Sweden, Tech. Rep. EAB-18 4510, Tech. Rep., 2017.

[6] A. Holst, *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030*, 2021. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide.

[7] L. Columbus, *2018 Roundup Of Internet Of Things Forecasts And Market Estimates*, 2018. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/.

[8] R. Sanchez-Iborra and M.-D. Cano, "State of the Art in LP-WAN Solutions for Industrial IoT Services", *Sensors*, vol. 16, no. 5, p. 708, 2016, ISSN: 1424-8220. DOI: 10.3390/s16050708. [Online]. Available: http://www.mdpi.com/1424-8220/16/5/708.

[9] S. Farrell, *Low-Power Wide Area Network (LPWAN) Overview*, RFC 8376, 2018. DOI: 10.17487/RFC8376. [Online]. Available: https://rfc-editor.org/rfc/rfc8376.txt.

[10] Chaudhari and Zennaro, *LPWAN Technologies for IoT and M2M Applications*. Elsevier, 2020, ISBN: 9780128188804. DOI: 10.1016/C2018-0-04787-8. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/C20180047878.

[11] J.-P. Bardyn, T. Melly, O. Seller, and N. Sornin, "IoT: The era of LPWAN is starting now", in *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, IEEE, 2016, pp. 25–30, ISBN: 978-1-5090-2972-3. DOI: 10.1109/ESSCIRC.2016.7598235. [Online]. Available: http://ieeexplore.ieee.org/document/7598235/.

[12] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment", *ICT Express*, vol. 5, no. 1, pp. 1–7, 2019, ISSN: 24059595. DOI: 10.1016/j.icte.2017.12.005. [Online]. Available: https://doi.org/10.1016/j.icte.2017.12.005.

[13] M. Bembe, A. Abu-Mahfouz, M. Masonta, and T. Ngqondi, "A survey on low-power wide area networks for IoT applications", *Telecommunication Systems*, vol. 71, no. 2, pp. 249–274, 2019, ISSN: 1018-4864. DOI: 10.1007/s11235-019-00557-9. [Online]. Available: https://doi.org/10.1007/s11235-019-00557-9http://link.springer.com/10.1007/s11235-019-00557-9.

[14] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview", *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017, ISSN: 1553-877X. DOI: 10.1109/COMST.2017.2652320. [Online]. Available: http://ieeexplore.ieee.org/document/7815384/.

[15] A. Minaburo, L. Toutain, C. Gomez, and D. Barthel, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", Tech. Rep. 8724, 2020. DOI: 10.17487/RFC8724. [Online]. Available: https://rfc-editor.org/rfc/rfc8724.txthttps://www.rfc-editor.org/info/rfc8724.

[16] Sigfox, *SIGFOX One Network A Billion Dreams. M2M and IoT Redefined Through Cost Effective and Energy Optimized Connectivity.* [Online]. Available: https://lafibre.info/images/3g/201302_sigfox_whitepaper.pdf.

[17] LoRa Alliance™, "What is it LoRaWAN™ - A technical overview of LoRa ® and LoRaWAN™", Tech. Rep. November, 2015. [Online]. Available: https://lora-alliance.org/resource-hub/what-lorawantm.

[18] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, and J.-P. Koskinen, "Overview of narrowband IoT in LTE Rel-13", in *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*, IEEE, 2016, pp. 1–7, ISBN: 978-1-5090-3862-6. DOI: 10.1109/CSCN.2016.7785170. [Online]. Available: http://ieeexplore.ieee.org/document/7785170/.

[19] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication", in *2016 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Doha, Qatar: IEEE, 2016, pp. 428–432, ISBN: 978-1-4673-8666-1. DOI: 10.1109/WCNCW.2016.7552737. [Online]. Available: http://ieeexplore.ieee.org/document/7552737/.

[20] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A Primer on 3GPP Narrowband Internet of Things", *IEEE Communications Magazine*, vol. 55, no. 3, pp. 117–123, 2017, ISSN: 0163-6804. DOI: 10.1109/MCOM.2017.1600510CM. arXiv: 1606.04171. [Online]. Available: http://ieeexplore.ieee.org/document/7876968/.

[21] Y. D. Beyene, R. Jantti, O. Tirkkonen, K. Ruttik, S. Iraji, A. Larmo, T. Tirronen, and T. Johan, "NB-IoT Technology Overview and Experience from Cloud-RAN Implementation", *IEEE Wireless Communications*, vol. 24, no. 3, pp. 26–32, 2017, ISSN: 1536-1284. DOI: 10.1109/MWC.2017.1600418. [Online]. Available: http://ieeexplore.ieee.org/document/7955908/.

[22] J Schlienz and D Raddino, "Narrowband Internet of Things Whitepaper", p. 42, 2016. [Online]. Available: https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma266/1MA266_0e_NB_IoT.pdf.

[23] D. Spence, G. Gross, C. de Laat, S. Farrell, L. H. M. Gommans, P. R. Calhoun, M. Holdrege, B. W. de Bruijn, and J. Vollbrecht, *AAA Authorization Framework*, RFC 2904, 2000. DOI: 10.17487/RFC2904. [Online]. Available: https://rfc-editor.org/rfc/rfc2904.txt.

[24] M. Nakhjiri and M. Nakhjiri, *AAA and Network Security for Mobile Access.* Chichester, UK: John Wiley & Sons, Ltd, 2005, ISBN: 9780470017463. DOI: 10.1002/0470017465. [Online]. Available: http://doi.wiley.com/10.1002/0470017465.

[25] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)", Tech. Rep., 2014. DOI: 10.17487/rfc7252. [Online]. Available: https://www.rfc-editor.org/info/rfc7252.

[26] O. Garcia-Morchon, S. Kumar, and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges", Tech. Rep., 2019, pp. 5–10. DOI: 10.17487/RFC8576. [Online]. Available: https://www.rfc-editor.org/info/rfc8576.

[27] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", Tech. Rep., 2007. DOI: 10.17487/rfc4919. [Online]. Available: https://www.rfc-editor.org/info/rfc4919.

[28] L.-E. Jonsson, K. Sandlund, and G. Pelletier, *The RObust Header Compression (ROHC) Framework*, RFC 5795, 2010. DOI: 10.17487/RFC5795. [Online]. Available: https://rfc-editor.org/rfc/rfc5795.txt.

[29] P. Thubert, J. Hui, J. Huji, and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", *Statewide Agricultural Land Use Baseline 2015*, Request for Comments, no. 6282, 2011, ISSN: 1098-6596. DOI: 10.1017/CBO9781107415324.004. arXiv: arXiv:1011.1669v3. [Online]. Available: https://rfc-editor.org/rfc/rfc6282.txt.

[30] G. Montenegro, J. Hui, D. Culler, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", Request for Comments, no. 4944, 2007, ISSN: 1098-6596. DOI: 10.23943/9781400889877. arXiv: arXiv:1011.1669v3. [Online]. Available: http://link.springer.com/10.1007/s11575-008-0104-y%5Cnhttp://www.palgrave-journals.com/doifinder/10.1057/jibs.2009.24%5Cnhttp://linkinghub.elsevier.com/retrieve/pii/S0925527313002028%5Cnhttp://www.palgrave-journals.com/doifinder/10.1057/palgrave.jibs.8400.

[31] R. Marin-Lopez, F. Pereniguez-Garcia, A. Gomez-skarmeta, and Y. Ohba, "Network access security for the internet: protocol for carrying authentication for network access", *IEEE Communications Magazine*, vol. 50, no. 3, pp. 84–92, 2012, ISSN: 0163-6804. DOI: 10.1109/MCOM.2012.6163586. [Online]. Available: http://ieeexplore.ieee.org/document/6163586/.

[32] D. Garcia-Carrillo, R. Marin-Lopez, A. Kandasamy, and A. Pelov, "A CoAP-Based Network Access Authentication Service for Low-Power Wide Area Networks: LO-CoAP-EAP", *Sensors*, vol. 17, no. 11, p. 2646, 2017, ISSN: 1424-8220. DOI: 10.3390/s17112646. [Online]. Available: http://www.mdpi.com/1424-8220/17/11/2646.

[33] B. Aboba, L. Blunk, J. Vollbrecht, and J. Carlson, "Extensible Authentication Protocol (EAP)", Tech. Rep., 2004. DOI: 10.17487/rfc3748. [Online]. Available: https://www.rfc-editor.org/info/rfc3748.

[34] B. Aboba, D Simon, and P Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", Tech. Rep., 2008. DOI: 10.17487/rfc5247. [Online]. Available: https://rfc-editor.org/rfc/rfc5247.txthttps://www.rfc-editor.org/info/rfc5247.

[35] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", Internet Engineering Task Force, Internet-Draft draft-ietf-ace-oauth-authz-43, 2021. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-ace-oauth-authz-43.

[36] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010, ISSN: 13891286. DOI: 10.1016/j.comnet.2010.05.010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010.

[37] J. Shalf, "The future of computing beyond Moore's Law", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 378, no. 2166, p. 20 190 061, 2020, ISSN: 1364-503X. DOI: 10.1098/rsta.2019.0061. [Online]. Available: https://royalsocietypublishing.org/doi/10.1098/rsta.2019.0061.

[38] WIRED UK, *Shenzhen: The Silicon Valley of Hardware - Documentary.* [Online]. Available: https://www.youtube.com/watch?v=SGJ5cZnoodY (visited on 08/22/2021).

[39] J. Salmeron-Garcia, P. Inigo-Blasco, F. Diaz-del Rio, and D. Cagigas-Muniz, "A Tradeoff Analysis of a Cloud-Based Robot Navigation Assistant Using Stereo Image Processing", *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 2, pp. 444–454, 2015, ISSN: 1545-5955. DOI: 10.1109/TASE.2015.2403593. [Online]. Available: http://ieeexplore.ieee.org/document/7052418/.

[40] C. Bormann, M. Ersue, and A. Keranen, "Terminology for Constrained-Node Networks", Tech. Rep. 7228, 2014. DOI: 10.17487/rfc7228. [Online]. Available: https://rfc-editor.org/rfc/rfc7228.txthttps://www.rfc-editor.org/info/rfc7228.

[41] M. Saelens, J. Hoebeke, A. Shahid, and E. D. Poorter, "Impact of EU duty cycle and transmission power limitations for sub-GHz LPWAN SRDs: an overview and future challenges", *Eurasip Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019, ISSN: 16871499. DOI: 10.1186/s13638-019-1502-5.

[42] R. K. Singh, P. P. Puluckul, R. Berkvens, and M. Weyn, "Energy Consumption Analysis of LPWAN Technologies and Lifetime Estimation for IoT Application", *Sensors*, vol. 20, no. 17, p. 4794, 2020, ISSN: 1424-8220. DOI: 10.3390/s20174794. [Online]. Available: https://www.mdpi.com/1424-8220/20/17/4794.

[43] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low Power Wide Area Networks: A Survey of Enabling Technologies, Applications and Interoperability Needs", *IEEE Access*, vol. 6, pp. 77 454–77 473, 2018, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2883151. [Online]. Available: https://ieeexplore.ieee.org/document/8550663/.

[44] European Parliament, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, 2016. [Online]. Available: http://data.europa.eu/eli/dir/2016/1148/oj (visited on 04/12/2021).

[45] ——, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da", *OJ*, vol. L 119, pp. 1,88, 2016. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj.

[46] ——, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52*, 2019. [Online]. Available: http://data.europa.eu/eli/reg/2019/881/oj (visited on 04/12/2021).

[47] E. Migabo, K. Djouani, and A. Kurien, "An Energy-Efficient and Adaptive Channel Coding Approach for Narrowband Internet of Things (NB-IoT) Systems", *Sensors*, vol. 20, no. 12, p. 3465, 2020, ISSN: 1424-8220. DOI: 10.3390/s20123465. [Online]. Available: https://www.mdpi.com/1424-8220/20/12/3465.

[48] H. Wu, C. Chen, and K. Weng, "An Energy-Efficient Strategy for Microcontrollers", *Applied Sciences*, vol. 11, no. 6, p. 2581, 2021, ISSN: 2076-3417. DOI: 10.3390/app11062581. [Online]. Available: https://www.mdpi.com/2076-3417/11/6/2581.

[49] R. Kufakunesu, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on adaptive data rate optimization in lorawan: Recent solutions and major challenges", *Sensors (Switzerland)*, vol. 20, no. 18, pp. 1–25, 2020, ISSN: 14248220. DOI: 10.3390/s20185044.

[50] H. Hellaoui, M. Koudil, and A. Bouabdallah, *Energy-efficient mechanisms in security of the internet of things: A survey*, 2017. DOI: 10.1016/j.comnet.2017.08.006.

[51] Open Mobile Alliance, *Lightweight Machine to Machine Technical Specification - LwM2M*, 2020. [Online]. Available: http://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-TS-LightweightM2M_Core-V1_2-20201110-A.pdf.

[52] ——, *Lightweight Machine to Machine - LwM2M v1.1*, 2019. [Online]. Available: http://www.openmobilealliance.org/release/LightweightM2M/Lightweight_Machine_to_Machine-v1_1-OMASpecworks.pdf.

[53] C. Bormann and P. Hoffman, "Concise Binary Object Representation (CBOR)", Tech. Rep., 2013. DOI: 10.17487/rfc7049. [Online]. Available: https://www.rfc-editor.org/info/rfc7049.

[54] G Selander, J Mattsson, F Palombini, and L Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, 2019. DOI: 10.17487/RFC8613. [Online]. Available: http://tools.ietf.org/rfc/rfc8613.txthttps://www.rfc-editor.org/info/rfc8613.

[55] E. Rescorla, H. Tschofenig, and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Internet Engineering Task Force, Internet-Draft draft-ietf-tls-dtls13-43, 2021. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-tls-dtls13-43.

[56] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", Tech. Rep., 2017. DOI: 10.17487/RFC8200. [Online]. Available: https://www.rfc-editor.org/info/rfc8200.

[57] T. Bray, *The JavaScript Object Notation (JSON) Data Interchange Format*, RFC 7159, 2014. DOI: 10.17487/RFC7159. [Online]. Available: https://rfc-editor.org/rfc/rfc7159.txt.

[58] L. Seitz, S. Gerdes, G. Selander, M. Mani, and S. Kumar, *Use Cases for Authentication and Authorization in Constrained Environments*, RFC 7744, 2016. DOI: 10.17487/RFC7744. [Online]. Available: https://rfc-editor.org/rfc/rfc7744.txt.

[59] J. Schaad, *CBOR Object Signing and Encryption (COSE)*, RFC 8152, 2017. DOI: 10.17487/RFC8152. [Online]. Available: https://rfc-editor.org/rfc/rfc8152.txthttps://www.rfc-editor.org/info/rfc8152.

[60] *OSCORE: A look at the new IoT security protocol - Ericsson*. [Online]. Available: https://www.ericsson.com/en/blog/2019/11/oscore-iot-security-protocol (visited on 06/27/2021).

[61] S. Thielemans, M. Bezunartea, and K. Steenhaut, "Establishing transparent IPv6 communication on LoRa based low power wide area networks (LPWANS)", in *2017 Wireless Telecommunications Symposium (WTS)*, IEEE, 2017, pp. 1–6, ISBN: 978-1-5090-3599-1. DOI: 10.1109/WTS.2017.7943535. [Online]. Available: http://ieeexplore.ieee.org/document/7943535/.

[62] P. Weber, D. Jackle, D. Rahusen, and A. Sikora, "IPv6 over LoRaWAN™", in *2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, IEEE, 2016, pp. 75–79, ISBN: 978-1-5090-4317-0. DOI: 10.1109/IDAACS-SWS.2016.7805790. [Online]. Available: http://ieeexplore.ieee.org/document/7805790/.

[63] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Santa, P. J. Fernández, and A. Skarmeta, "Integrating LP-WAN Communications within the Vehicular Ecosystem", in *The 2017 International Symposium on Mobile Internet Security (MobiSec'17)*, Jeju Island, Republic of Korea, 2017, pp. 1–12. DOI: 10.22667/JISIS.2017.11.30.045. [Online]. Available: http://doi.org/10.22667/JISIS.2017.11.30.045.

[64] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Santa, P. J. Fernandez, and A. F. Skarmeta, "IPv6 communications over LoRa for future IoV services", in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, vol. 2018-Janua, IEEE, 2018, pp. 92–97, ISBN: 978-1-4673-9944-9. DOI: 10.1109/WF-IoT.2018.8355231. [Online]. Available: https://ieeexplore.ieee.org/document/8355231/.

[65] P. Thubert, A. Pelov, and S. Krishnan, "Low-Power Wide-Area Networks at the IETF", *IEEE Communications Standards Magazine*, vol. 1, no. 1, pp. 76–79, 2017, ISSN: 2471-2825. DOI: 10.1109/MCOMSTD.2017.1600002ST. [Online]. Available: http://ieeexplore.ieee.org/document/7885244/.

[66] A Minaburo, C Gomez, L Toutain, J Paradells, J. Crowcroft, and G. A. P. Analysis, *LPWAN Survey and GAP Analysis*. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-minaburo-lpwan-gap-analysis-02.

[67] A. Minaburo, L. Toutain, and R. Andreasen, *Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)*, RFC 8824, 2021. DOI: 10.17487/RFC8824. [Online]. Available: https://rfc-editor.org/rfc/rfc8824.txt.

[68] C. Gomez, A. Minaburo, L. Toutain, D. Barthel, and J. C. Zuniga, "IPv6 over LPWANs: Connecting low power wide area networks to the internet (of Things)", *IEEE Wireless Communications*, vol. 27, no. 1, pp. 206–213, 2020, ISSN: 15580687. DOI: 10.1109/MWC.001.1900215.

[69] B. Moons, A. Karaagac, J. Haxhibeqiri, E. D. Poorter, and J. Hoebeke, "Using SCHC for an optimized protocol stack in multimodal LPWAN solutions", in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, IEEE, 2019, pp. 430–435, ISBN: 978-1-5386-4980-0. DOI: 10.1109/WF-IoT.2019.8767210. [Online]. Available: https://ieeexplore.ieee.org/document/8767210/.

[70] W. Ayoub, F. Nouvel, S. Hmede, A. E. Samhat, M. Mroue, and J.-C. Prevotet, "Implementation of SCHC in NS-3 and Comparison with 6LoWPAN", in *2019 26th International Conference on Telecommunications (ICT)*, IEEE, 2019, pp. 432–436, ISBN: 978-1-7281-0273-3. DOI: 10.1109/ICT.2019.8798782. [Online]. Available: https://ieeexplore.ieee.org/document/8798782/.

[71] A. Minaburo and L. Toutain, "Comparison of 6lo and SCHC", Internet Engineering Task Force, Internet-Draft draft-toutain-6lo-6lo-and-schc-00, 2019. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-toutain-6lo-6lo-and-schc-00.

[72] K. Q. Abdelfadeel, V. Cionca, and D. Pesch, "Dynamic Context for Static Context Header compression in LPWANs", in *2018 14th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, IEEE, 2018, pp. 35–42, ISBN: 978-1-5386-5470-5. DOI: 10.1109/DCOSS.2018.00013. [Online]. Available: https://ieeexplore.ieee.org/document/8510958/.

[73] A. Ludovici, A. Calveras, and J. Casademont, "Forwarding techniques for IP fragmented packets in a real 6LoWPAN network", *Sensors*, vol. 11, no. 1, pp. 992–1008, 2011, ISSN: 14248220. DOI: 10.3390/s110100992.

[74] F. Mesrinejad, F. Hashim, N. K. Noordin, M. F. A. Rasid, and R. S. A. R. Abdullah, "The effect of fragmentation and header compression on IP-based sensor networks (6LoWPAN)", in *The 17th Asia Pacific Conference on Communications*, IEEE, 2011, pp. 845–849, ISBN: 978-1-4577-0390-4. DOI: 10.1109/APCC.2011.6152926. [Online]. Available: http://ieeexplore.ieee.org/document/6152926/.

[75] I. Suciu, X. Vilajosana, and F. Adelantado, "An analysis of packet fragmentation impact in LPWAN", in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, 2018, pp. 1–6, ISBN: 978-1-5386-1734-2. DOI: 10.1109/WCNC.2018.8377440. [Online]. Available: https://ieeexplore.ieee.org/document/8377440/.

[76] ——, "Aggressive Fragmentation Strategy for Enhanced Network Performance in Dense LPWANs", in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, vol. 2018-Septe, IEEE, 2018, pp. 1833–1838, ISBN: 978-1-5386-6009-6. DOI: 10.1109/PIMRC.2018.8581051. arXiv: 1901.11330. [Online]. Available: https://ieeexplore.ieee.org/document/8581051/.

[77] IEEE, *IEEE 802.1Qbu-2016 - IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks – Amendment 26: Frame Preemption*, 2016. [Online]. Available: https://standards.ieee.org/standard/802_1Qbu-2016.html.

[78] K. Q. Abdelfadeel, V. Cionca, and D. Pesch, "LSCHC: Layered Static Context Header Compression for LPWANs", in *Proceedings of the 12th Workshop on Challenged Networks - CHANTS '17*, New York, New York, USA: ACM Press, 2017, pp. 13–18, ISBN: 9781450351447. DOI: 10.1145/3124087.3124092. arXiv: 1708.05209. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3124087.3124092.

[79] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks", *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016, ISSN: 1553877X. DOI: 10.1109/COMST.2016.2548426.

[80] W. Zada Khan, Y. Xiang, M. Y Aalsalem, and Q. Arshad, "The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures", *International Journal of Wireless and Microwave Technologies*, vol. 2, no. 2, pp. 33–44, 2012, ISSN: 20761449. DOI: 10.5815/ijwmt.2012.02.06. [Online]. Available: http://www.mecs-press.org/ijwmt/ijwmt-v2-n2/v2n2-6.html.

[81] M. Sethi, B. Sarikaya, and D. Garcia-Carrillo, "Secure IoT Bootstrapping: A Survey", Internet Engineering Task Force, Internet-Draft draft-irtf-t2trg-secure-bootstrapping-00, 2021. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-secure-bootstrapping-00.

[82] J. Arkko, V. Lehtovirta, and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", Tech. Rep., 2009, pp. – 1699. DOI: 10.17487/rfc5448. [Online]. Available: https://www.rfc-editor.org/info/rfc5448.

[83] V. S. Miller, "Use of Elliptic Curves in Cryptography", in *Advances in Cryptology — CRYPTO '85 Proceedings*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 417–426. DOI: 10.1007/3-540-39799-X_31. [Online]. Available: http://link.springer.com/10.1007/3-540-39799-X_31.

[84] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, vol. 48, no. 177, pp. 203–203, 1987, ISSN: 0025-5718. DOI: 10.1090/S0025-5718-1987-0866109-5. [Online]. Available: http://www.ams.org/jourcgi/jour-getitem?pii=S0025-5718-1987-0866109-5.

[85] J. P. Mattsson, F. Palombini, and M. Vučinić, "Comparison of CoAP Security Protocols", Internet Engineering Task Force, Internet-Draft draft-ietf-lwig-security-protocol-comparison-05, 2020. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lwig-security-protocol-comparison-05.

[86] G. Selander, J. P. Mattsson, and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", Internet Engineering Task Force, Internet-Draft draft-ietf-lake-edhoc-09, 2021. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-lake-edhoc-09.

[87] D. Chandramouli, R. Liebhart, J. Pirskanen, G Choudhary, J Kim, and V Sharma, "5G for the Connected World", *Wiley*, vol. 9, no. 4, pp. –, 2019. DOI: 10.1002/9781119247111.

[88] 3GPP, "3GPP TS 22.261 Service requirements for the 5G system Stage 1 Release 16", vol. 0, no. Release 16.2.0, 2019.

[89] NGMN Alliance, "5G White Paper", Tech. Rep., 2015. [Online]. Available: https://www.ngmn.org/work-programme/5g-white-paper.html.

[90] 3GPP, T. Specification, and G. Services, "System architecture for the 5G System (5GS). Technical Specification (TS) 23.501, 3rd Generation Partnership Project", vol. 0, no. Release 16, p. 16 1 0, 2020.

[91] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond", *IEEE Communications Surveys & Tutorials*, no. May, pp. 1–1, 2019, ISSN: 1553-877X. DOI: 10.1109/comst.2019.2916180.

[92] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions", *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018, ISSN: 2471-2825. DOI: 10.1109/MCOMSTD.2018.1700063. [Online]. Available: https://ieeexplore.ieee.org/document/8334918/.

[93] A. Kunz and X. Zhang, "New 3GPP Security Features in 5G Phase 1", *2018 IEEE Conference on Standards for Communications and Networking, CSCN 2018*, no. October, 2018. DOI: 10.1109/CSCN.2018.8581763.

[94] F. Al-Turjman, E. Ever, and H. Zahmatkesh, "Small Cells in the Forthcoming 5G/IoT: Traffic Modelling and Deployment Overview", *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 28–65, 2019, ISSN: 1553-877X. DOI: 10.1109/COMST.2018.2864779. [Online]. Available: https://ieeexplore.ieee.org/document/8430735/.

[95] ITU, "Minimum requirements related to technical performance for IMT-2020 radio interface(s)", *Working Party 5D*, vol. November, no. 5D/TEMP/300(Rev.1), pp. 1–148, 2017. [Online]. Available: https://www.itu.int/pub/R-REP-M.2410-2017.

[96] R. P. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions", *International Symposium on Wireless Personal Multimedia Communications, WPMC*, 2013, ISSN: 13476890. [Online]. Available: https://ieeexplore.ieee.org/document/6618585.

[97] 3GPP and G.P.P., "Security Architecture and Procedures for 5G System. Technical Specification (TS) 33.501, 3rd Generation Partnership Project (3GPP). Release 16", vol. 0, no. Release 15.4.0, 2019. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501.

[98] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol", Tech. Rep., 2008. DOI: 10.17487/rfc5216. [Online]. Available: https://www.rfc-editor.org/info/rfc5216.

[99] CableLabs, *A Comparative Introduction to 4G and 5G Authentication*, 2019. [Online]. Available: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication.

[100] 5GPPP Architecture Working Group, "view on 5G architecture", *White Paper*, no. June, 2019. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2018/01/5G-PPP-5G-Architecture-White-Paper-Jan-2018-v2.0.pdf.

[101] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What Will 5G Be?", *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014, ISSN: 0733-8716. DOI: 10.1109/JSAC.2014.2328098. arXiv: arXiv:1405.2957v1. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6824752.

[102] M. Condoluci, S. H. Johnson, V. Ayadurai, M. A. Lema, M. A. Cuevas, M. Dohler, and T. Mahmoodi, "Fixed-Mobile Convergence in the 5G Era: From Hybrid Access to Converged Core", *IEEE Network*, vol. 33, no. 2, pp. 138–145, 2019, ISSN: 0890-8044. DOI: 10.1109/MNET.2018.1700462. [Online]. Available: https://ieeexplore.ieee.org/document/8637090/.

[103] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", Tech. Rep. 7296, 2014. DOI: 10.17487/rfc7296. [Online]. Available: https://rfc-editor.org/rfc/rfc7296.txthttps://www.rfc-editor.org/info/rfc7296.

[104] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", Tech. Rep., 2005. DOI: 10.17487/rfc4301. [Online]. Available: https://www.rfc-editor.org/info/rfc4301.

[105] D. Garcia-Carrillo and R. Marin-Lopez, "Lightweight CoAP-based bootstrapping service for the internet of things", *Sensors (Switzerland)*, vol. 16, no. 3, p. 358, 2016, ISSN: 14248220. DOI: 10.3390/s16030358.

[106] R. Marin-Lopez and D. Garcia-Carrillo, "EAP-based Authentication Service for CoAP", Internet Engineering Task Force, Internet-Draft draft-ietf-ace-wg-coap-eap-03, 2021. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-ace-wg-coap-eap-03.

[107] A. Bhattacharyya, S. Bandyopadhyay, A. Pal, and T. Bose, "Constrained Application Protocol (CoAP) Option for No Server Response", Tech. Rep., 2016. DOI: 10.17487/RFC7967. [Online]. Available: a/index.php/ae/article/view/106https://www.rfc-editor.org/info/rfc7967.

[108] A. Rubens, C. Rigney, S. Willens, and W. A. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, RFC 2865, 2000. DOI: 10.17487/RFC2865. [Online]. Available: https://rfc-editor.org/rfc/rfc2865.txt.

[109] V. Fajardo, J. Arkko, J. A. Loughney, and G. Zorn, *Diameter Base Protocol*, RFC 6733, 2012. DOI: 10.17487/RFC6733. [Online]. Available: https://rfc-editor.org/rfc/rfc6733.txt.

[110] F. Bersani and H. Tschofenig, *The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method*, RFC 4764, 2007. DOI: 10.17487/rfc4764. [Online]. Available: https://rfc-editor.org/rfc/rfc4764.txthttps://www.rfc-editor.org/info/rfc4764.

[111] D. Forsberg, B. Patil, H. Tschofenig, and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", Tech. Rep., 2008. DOI: 10.17487/rfc5191. [Online]. Available: https://www.rfc-editor.org/info/rfc5191.

[112] L. Alliance, N Sornin, M Luis, T Eirich, T Kramp, and O Hersent, "LoRaWAN ™ Specification v1.0.2", *LoRa™ Alliance*, 2016. [Online]. Available: https://lora-alliance.org/resource-hub/lorawantm-specification-v102.

[113] L. A. T. Committee, "LoRaWAN™ 1.0.2 Regional Parameters", Tech. Rep., 2017, pp. 1–55. [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_regional_parameters_v1.0.2_final_1944_1.pdf.

[114] Semtech, "LoRa Modulation Basics AN1200.22", *App Note*, no. May, pp. 1–26, 2015. [Online]. Available: http://www.semtech.com/images/datasheet/an1200.22.pdf.

[115] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Viñas, M.-D. Cano, and A. Skarmeta, "Performance Evaluation of LoRa Considering Scenario Conditions", *Sensors*, vol. 18, no. 3, p. 772, 2018, ISSN: 1424-8220. DOI: 10.3390/s18030772. [Online]. Available: http://www.mdpi.com/1424-8220/18/3/772.

[116] K. Q. Abdelfadeel, V. Cionca, and D. Pesch, "Fair Adaptive Data Rate Allocation and Power Control in LoRaWAN", in *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, IEEE, 2018, pp. 14–15, ISBN: 978-1-5386-4725-7. DOI: 10.1109/WoWMoM.2018.8449737. arXiv: 1802.10338. [Online]. Available: https://ieeexplore.ieee.org/document/8449737/.

[117] R. Sanchez-Iborra and A. F. Skarmeta, "TinyML-Enabled Frugal Smart Objects: Challenges and Opportunities", *IEEE Circuits and Systems Magazine*, vol. 20, no. 3, pp. 4–18, 2020, ISSN: 1531-636X. DOI: 10.1109/MCAS.2020.3005467. [Online]. Available: https://ieeexplore.ieee.org/document/9166461/.

[118] R. Sanchez-Iborra, "LPWAN and Embedded Machine Learning as Enablers for the Next Generation of Wearable Devices", *Sensors*, vol. 21, no. 15, p. 5218, 2021, ISSN: 1424-8220. DOI: 10.3390/s21155218. [Online]. Available: https://www.mdpi.com/1424-8220/21/15/5218.

5.1. Publications

[119] J. Sanchez-Gomez, D. G. Carrillo, R. Sanchez-Iborra, J. L. Hernandez-Ramos, J. Granjal, R. Marin-Perez, and M. A. Zamora-Izquierdo, "Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions", *IEEE Access*, vol. 8, pp. 216 437–216 460, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3041057. [Online]. Available: https://ieeexplore.ieee.org/document/9272765/.

[120] J. Sanchez-Gomez, J. Gallego-Madrid, R. Sanchez-Iborra, J. Santa, and A. Skarmeta, "Impact of SCHC Compression and Fragmentation in LPWAN: A Case Study with LoRaWAN", *Sensors*, vol. 20, no. 1, p. 280, 2020, ISSN: 1424-8220. DOI: 10.3390/s20010280. [Online]. Available: https://www.mdpi.com/1424-8220/20/1/280.

[121] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, and A. F. Skarmeta, "Secure Authentication and Credential Establishment in Narrowband IoT and 5G", *Sensors*, vol. 20, no. 3, p. 882, 2020, ISSN: 1424-8220. DOI: 10.3390/s20030882. [Online]. Available: https://www.mdpi.com/1424-8220/20/3/882.

[122] J. Sanchez-Gomez, J. Gallego-Madrid, R. Sanchez-Iborra, and A. F. Skarmeta, "Performance Study of LoRaWAN for Smart-City Applications", in *2019 IEEE 2nd 5G World Forum (5GWF)*, IEEE, 2019, pp. 58–62, ISBN: 978-1-7281-3627-1. DOI: 10.1109/5GWF.2019.8911676. [Online]. Available: https://ieeexplore.ieee.org/document/8911676/.

[123] R. Sanchez-Iborra, S. Covaci, J. Santa, J. Sanchez-Gomez, J. Gallego-Madrid, and A. F. Skarmeta, "MEC-Assisted End-to-End 5G-Slicing for IoT", in *2019 IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2019, pp. 1–6, ISBN: 978-1-7281-0962-6. DOI: 10.1109/GLOBECOM38437.2019.9013623. [Online]. Available: https://ieeexplore.ieee.org/document/9013623/.

[124] D. Garcia-Carrillo, J. Sanchez-Gomez, R. Marin-Perez, and A. Skarmeta, "EAP-Based Bootstrapping for Secondary Service Authentication to Integrate IoT into 5G Networks", in *Communications in Computer and Information Science*, 7, vol. 1121, 2020, pp. 13–22, ISBN: 9789811596087. DOI: 10.1007/978-981-15-9609-4_2. [Online]. Available: http://link.springer.com/10.1007/978-981-15-9609-4_2.

[125] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, R. Sanchez-Iborra, and A. F. S. Gomez, "Secure bootstrapping and header compression for IoT constrained networks", in *GIoTS 2020 - Global Internet of Things Summit, Proceedings*, IEEE, 2020, pp. 1–6, ISBN: 9781728121710. DOI: 10.1109/GIOTS49054.2020.9119644. [Online]. Available: https://ieeexplore.ieee.org/document/9119644/.

[126] J. Sanchez-Gomez, R. Marin-Perez, M. Ross, and A. F. Skarmeta, "Holistic IoT Architecture for Secure Lightweight Communication, Firmware Update, and Trust Monitoring", in *2021 IEEE International Conference on Smart Internet of Things (SmartIoT)*, IEEE, 2021. DOI: 10.1109/SmartIoT52359.2021.00066. [Online]. Available: http://doi.org/10.1109/SmartIoT52359.2021.00066.

[127] J. Sanchez-Gomez, R. Marin-Perez, R. Sanchez-Iborra, and M. A. Zamora, "MEC-based Architecture for Interoperable and Trustworthy Internet of Moving Things", *Digital Communications and Networks(DCN)*, In press.