Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things

Jorge Navarro-Ortiz, Sandra Sendra, Pablo Ameigeiras, and Juan M. Lopez-Soler

The authors propose a solution to seamlessly integrate LoRaWAN, an open and standardized LPWAN technology, with 4G/5G mobile networks, thus allowing mobile network operators to reutilize their current infrastructures. This proposal is transparent to LoRaWAN end devices and to the EPC, since only the LoRaWAN gateway needs to be modified.

Abstract

Current forecasts predict that the Industrial Internet of Things will account for about 10 billion devices by 2020. Simultaneously, unlicensed low-power wide area networks are gaining momentum due to their low cost, low power, and long range characteristics, which are suitable for many IIoT applications, in addition to the usage of unlicensed bands. In this article, a solution is proposed to seamlessly integrate LoRaWAN, an open and standardized LPWAN technology, with 4G/5G mobile networks, thus allowing mobile network operators to reutilize their current infrastructures. This proposal is transparent to LoRaWAN end devices and to the EPC, since only the LoRaWAN gateway needs to be modified. The gateway acts as an evolved Node B from the core network perspective, implementing part of the eNB protocol stack. All data packets transported over the core network are both encrypted and integrity protected, hence achieving end-to-end security. As a proof of concept, this solution has been implemented and validated with an open source EPC.

Introduction

The Internet of Things (IoT) is one of the hottest topics in communications today. Although the forecast of 50 billion devices by 2020 may be outdated, the general trend that early analysts predicted is undeniable. Current values vary from 6 to 9 billion devices, whereas forecasts estimate from 20 to 30 billion IoT devices for 2020 (e.g., Ericsson's figure is 28 billion for 2021) [1]. Gartner [2] has forecast that Industrial IoT (IIoT) devices will represent around 37 percent of the global number, which will account for about 57 percent of overall IoT spending in 2017.

Although there is no formal definition [3], an IEEE report describes IoT as *"a network of items — each embedded with sensors — which are connected to the Internet."* Considering the type and the purpose of the things connected, IoT systems can be classified into *consumer*, *industrial*, and *manufacturing*.

Consumer IoT systems connect things that consumers utilize such as wearable devices, home automation, and security devices, or for healthcare. Their purpose is to improve the users' quality of life. Industrial IoT systems connect things that basically are non-consumer (i.e., things used by professionals and companies). IIoT use cases encompass industrial machinery, transportation monitoring, logistic tracking, asset tracking, healthcare, intelligent buildings, smart cities, smart agriculture, and smart metering. Their purpose is to increase productivity and reduce the environmental impact. *Manufacturing IoT systems* are focused on factories in order to optimize their processes (*smart manufacturing*).

The precise industries that are covered under IIoT depend on the approach of the different industry bodies. For example, in many cases the terms Industrie 4.0 and IIoT are used interchangeably, but the former is restricted to manufacturing.[1] However, the Industrial Internet[2] Consortium considers the following industries as the major IIoT vertical markets: energy, healthcare, manufacturing, smart cities, and transportation.

Many of these IIoT use cases can be considered as massive machine-type communications (mMTC), one of the three major fifth generation (5G) use cases (in addition to enhanced mobile broadband, and ultra-reliable and lowlatency MTC). For mMTC, there are two technologies that meet the low power and wide area requirements of these applications: cellular evolution and low-power wide area networks (LPWANs).

The Third Generation Partnership Project (3GPP) efforts try to leverage existing mobile networks for providing cellular IoT connectivity in order to avoid the maintenance and operation of a parallel network. The cellular IoT standardization proposes complete integration with mobile network operator (MNO) networks.

Although previous cellular standards have been used for MTC communications, they are not specifically suitable for mMTC services due to high cost and high power consumption. Specifically, based on these standards, 3GPP has defined the following schemes: Extended Coverage Global System for Mobile Communications (EC-GSM), LTE Cat-0 (a new low-complexity Long Term Evolution user equipment, UE, category 0, defined in 3GPP Release 12), LTE-M (also known as Cat-M1), and narrowband IoT (NB-IoT, also known as Cat-M2).

The advantage of both LTE Cat0 and LTE-M is that they are compatible with existing LTE networks. NBIoT addresses the requirements of mMTC, but utilizes a different radio technology (DSSS modulation), so it requires a specific frequency band (e.g., using dedicated spectrum, refarming GSM channels, or utilizing some resource blocks within a normal LTE carrier).

[1] Industrie 4.0 is a term coined by the German Federal Government to optimize industrial production and provide smart manufacturing solutions.

[2] Industrial Internet is a term coined by General Electric (GE), one of the founding members of the Industrial Internet Consortium. According to GE, the Industrial Internet of Things, also known as the Industrial Internet, is defined as "an internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes."

Digital Object Identifier: 10.1109/MCOM.2018.1700625

The authors are with the University of Granada.

The first trials of these technologies started at the end of 2016, launching the first deployments in 2017.

LPWANs try to cover the gap between traditional cellular technologies and current mMTC requirements. Local and mesh networks can fulfill many requirements such as low battery consumption and optimization for low data transfers, but they cannot offer global area coverage. Examples of LPWAN technologies are LoRaWAN, SigFox, RPMA, and NWave. They offer long range (up to several tens of kilometers), very low power consumption (years of battery operation), and very low bandwidth (tens of kilobits per second), and utilize license-exempt frequency bands.

Most LPWAN technologies have much lower cost compared to traditional cellular networks. This fact allows new players to assume the role of network operators, thus competing with current MNOs. Studies such as [4] predict that LPWANs will generate revenues of US$23 billion by 2020, so MNOs will be highly motivated to regain the market. For this reason, many MNOs (KPN, Orange, SK Telecom, Bouygues Telecom, Swisscom, SoftBank, etc.) have started to deploy LoRaWAN networks to complement their current cellular networks.

In this article, we devise a novel solution to seamlessly integrate LoRaWAN with the core network of a 4G/5G mobile network, that is, with an Evolved Packet Core (EPC). Our solution will allow MNOs to reutilize their existing infrastructures with minimum investment, and to easily integrate this service into their operation and maintenance (O&M) platforms. Additionally, end-to-end security is ensured between the LoRaWAN devices and the application servers. Although this work is focused on LoRaWAN, many of the ideas could be applied to other types of LPWAN. We selected LoRaWAN due to its excellent features, such as very low cost (for both end devices and infrastructure), very low power consumption, very long range, bidirectional communications, and high security.

The rest of the article is organized as follows. First, we present previous works. LoRaWAN is then described. Next, LoRaWAN and LTE security aspects are summarized, respectively. We explain our proposal for LoRaWAN and 4G/5G mobile networks integration. As a proof of concept, the main issues of the developed prototype are presented, and finally, we conclude the article.

Previous Works

To the best of the authors' knowledge, there are no other proposals to integrate LoRaWAN (or other unlicensed LPWAN technologies) with 3GPP mobile networks.

However, other solutions to integrate Wi-Fi into LTE have been proposed. The purpose of this integration is different from our proposal since the usage of Wi-Fi is intended to offload traffic, increasing the data rates, reducing the interference on the cellular network, and saving on costs. Wi-Fi is particularly interesting to MNOs since, according to the latest Cisco global mobile data forecast, 63 percent of the total mobile data traffic was offloaded through Wi-Fi or small cells in 2016.

For this purpose, 3GPP has defined two WLAN interworking features in Release 13: LTE-WLAN aggregation (LWA) and LTE WLAN radio-level integration with IPsec tunnel (LWIP).

LWA aggregates LTE and WLAN at the radio access network (RAN) level by allowing WLAN access points to only interact with the LTE evolved Node B (eNB), that is, without interaction with the EPC. This approach eliminates the need for WLAN-specific core network nodes. The integration is done by using a single bearer that utilizes both LTE and WLAN simultaneously. However, in Release 13 LWA only supports aggregation in the downlink, so uplink transmissions are always sent over LTE. Downlink packets are encapsulated in the LWA Adaptation Protocol (LWAAP), and user plane split/switch between LTE and WLAN is done at the Packet Data Convergence Protocol (PDCP) level.

If the eNB and the access point are not co-located, a new interface Xw is required for both control and user planes, connecting them through a WLAN termination (WT). The communication between the WT and the access points is out of 3GPP's scope.

Although the WLAN payload is encrypted by PDCP, 3GPP utilizes WLAN security including encryption, authentication, and protection using Extensible Authentication Protocol for the Third Generation Authentication and Key Agreement (EAP/AKA) or an optional optimized authentication.

For mobility, the eNB configures the WLAN mobility set (group of access points), but mobility within a WLAN is controlled by the UE (not by the eNB).

In LWIP, the UE uses WLAN over an IPsec tunnel between the UE and the eNB (establishing a connection to a specific secure gateway, LWIP-SeGW, using Internet key exchange, IKE, after the association and EAP/AKA authentication). The IPsec tunnel is transparent to the WLAN infrastructure, which is not modified. In addition, the WLAN is hidden from the EPC except for authentication. Both uplink and downlink communications are possible over a WLAN, and multiple bearers can be offloaded via IPsec. Both measurement reporting and WLAN mobility are reused from LWA.

LWA and LWIP architectures and related protocols are depicted in Fig. 1.

The main differences between LWA and LWIP from the end-user perspective is that LWA uses WLAN only for downlink traffic, but allows the use of WLAN and LTE simultaneously. In contrast, LWIP allows the user to transfer data over a WLAN for both uplink and downlink, but LTE is not used if the WLAN is active. In addition, fast/optimized WLAN authentication is not supported.

LWA and LWIP differ from our proposal both in purpose and required changes. On one hand, our solution integrates a LPWAN technology, -targeted for mMTC services with low power and low bandwidth requirements, whereas LWA and LWIP are technologies to offload mobile data traffic with high data rates. On the other hand, our solution does not require any changes to the existing mobile network, and no new protocols or signaling procedures are needed.

The main differences between LWA and LWIP from the end-user perspective is that LWA uses WLAN only for downlink traffic, but allows the usage of both WLAN and LTE simultaneously. In contrast, LWIP allows the user to transfer data over WLAN for both uplink and downlink, but LTE is not used if WLAN is active.

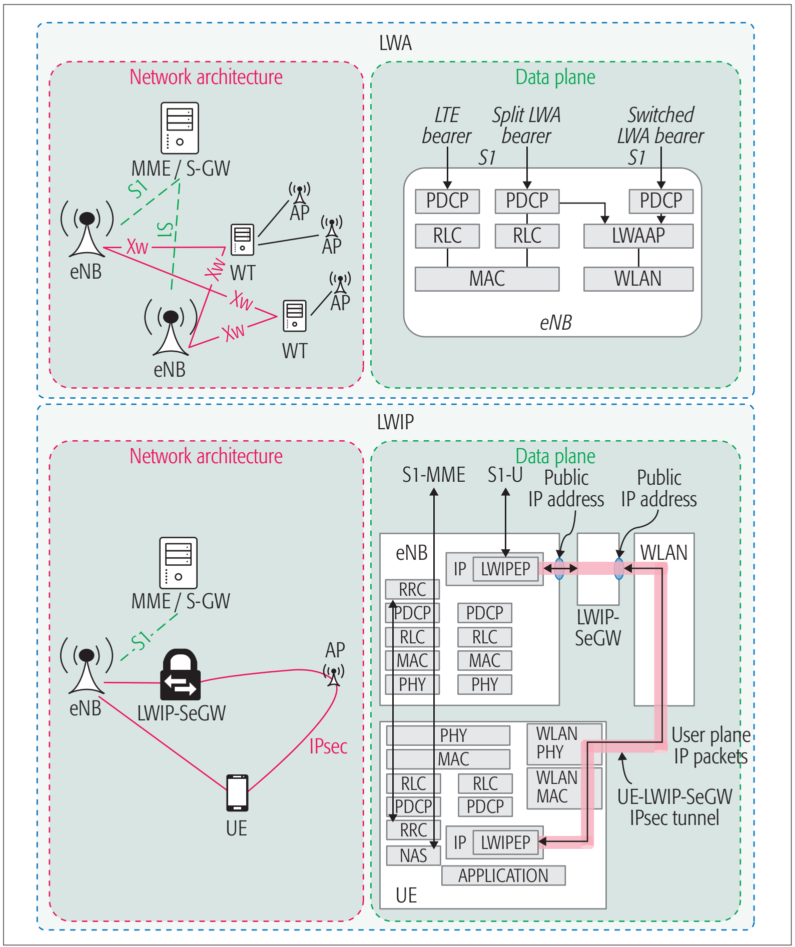


Figure 1. LWA and LWIP architecture and protocols [5].

LoRaWAN Specification

LoRaWAN [6] is an open and standardized LPWAN, which uses long range (LoRa) [7] or frequency shift keying (FSK) in the physical layer. LoRa modulation was developed by Cycleo, later acquired by Semtech. According to Semtech, the key features of this technology are low cost (in terms of infrastructure investment, operating expenses, and end devices), standardization (allowing interoperability), low power (extending battery lifetime up to 20 years), long range (deep penetration in dense urban/indoor regions, and up to 30 miles in rural areas), geolocation (GPS-free geolocation without requiring additional power), security (end-to-end AES Advanced Encryption Standard, AES, encryption) and high capacity (support of many devices per LoRaWAN gateway).

Unlike other IoT technologies, LoRaWAN does not use a mesh network architecture. Although mesh networking may be useful to increase the communication range, it also affects the device battery life due to the forwarding of messages. For that reason, LoRaWAN uses a star topology [6] in which devices are connected directly to gateways, which in turn are connected to a network server through a backhaul (e.g., Ethernet).

LoRaWAN allows end devices to have bidirectional communications, although they are asymmetric, since uplink transmissions (from end devices to gateways) are strongly favored. In this sense, there are three types of devices (Classes A, B, and C) defined in the standard, each with different capabilities [6]. Class A devices are typically battery powered sensors. This class is the most energy-efficient and must be supported by all devices, but the network can only transmit to the device after a data transmission from the device. For this, the device has to check for downlink transmissions during two receive windows. The second receive window is disabled after a successful transmission in the first window. This class is intended for energy-limited devices.

Class B allows devices to increase their downlink traffic and to reduce the latency for downlink communications (e.g. battery powered actuators). The gateway sends periodic beacons to synchronize these devices in order to schedule further receive windows (*ping slots*). The reception of downlink traffic increases the power requirement for these devices.

Finally, devices implementing Class C communications profiles are used for applications that have enough power available and can receive at any moment except during transmissions. Typical Class C devices are main powered actuators, which can afford to listen continuously and may require no latency for downlink communication.

Class A is mandatory for all end devices, and all devices must be compatible with this class. There can be devices from all the classes in a LoRaWAN network. The standard allows devices to change between classes (except Class C devices, which cannot implement Class B), although LoRaWAN does not define how to inform the gateway. Figure 2 depicts the LoRaWAN network architecture and the different device classes.

The underlying PHY layer for the three classes is the same. LoRa [7] is a proprietary spread spectrum modulation scheme which is based on chirp spread spectrum (CSS). Some of the key properties of this modulation are scalable bandwidth, constant envelope, low power, high robustness, multipath and fading resistant, Doppler resistant, long-range capability, enhanced network capacity, and geolocation capabilities.

Using different spreading factors (SFs), the developer may trade data rate for coverage or energy consumption. The spreading factor is defined as

$$SF = \log_2\left(\frac{R_C}{R_S}\right),$$

where R_S and R_C are the symbol and chip rates, respectively. The usage of a high SF decreases the data rate but increases the maximum distance between the transmitter and the receiver, and vice versa. Since transmissions using different SFs are orthogonal, it is possible to receive multiple frames simultaneously. LoRa error correction [7] reduces the bit rate by a factor rate code = 4/(4+CR), where code rate (CR) is an integer value between 1 and 4. According to [7], the bit rate can be computed as

$$Rb = SF \times \frac{\frac{4}{4+CR}}{\frac{2^{SF}}{BW}}.$$

Since SFs vary from 7 to 12 [8], and frames sent with different SFs can be decoded simultaneously,

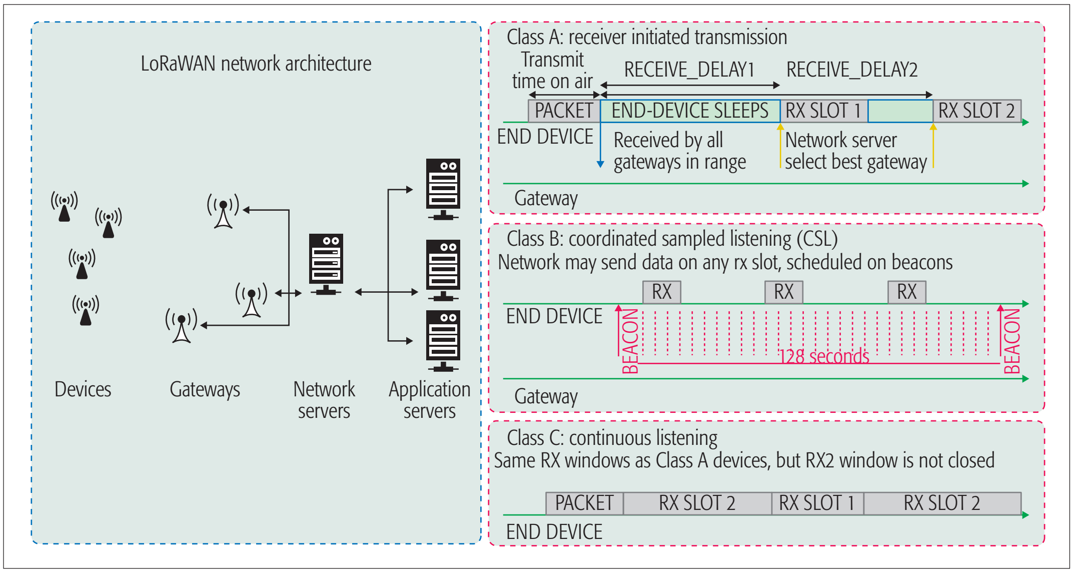

LoRaWAN network architecture
Devices
Gateways
Network servers
Application servers
Class A: receiver initiated transmission
Transmit time on air
RECEIVE_DELAY1
RECEIVE_DELAY2
PACKET
END-DEVICE SLEEPS
RX SLOT 1
RX SLOT 2
END DEVICE
Received by all gateways in range
Network server select best gateway
Gateway
Class B: coordinated sampled listening (CSL)
Network may send data on any rx slot, scheduled on beacons
RX
RX
RX
END DEVICE
BEACON
128 seconds
BEACON
Gateway
Class C: continuous listening
Same RX windows as Class A devices, but RX2 window is not closed
PACKET
RX SLOT 2
RX SLOT 1
RX SLOT 2
END DEVICE

Figure 2. LoRaWAN network and devices.

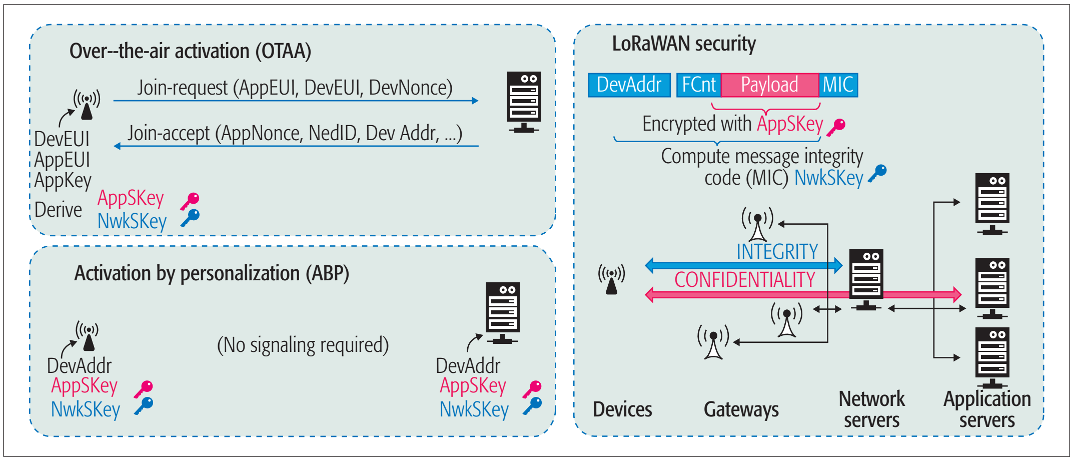


Figure 3. LoRaWAN security procedures.

Unlike other IoT technologies, LoRaWAN does not use a mesh network architecture. Although mesh networking may be useful to increase the communication range, it also affects the device battery life due to the forwarding of messages. For that reason, LoRaWAN uses a star topology.

the maximum aggregated bit rate (assuming *BW* = 500 kHz and *CR* = 1) is 43 kb/s. If FSK is used, the bit rate is 50 kb/s [8].

The channel bandwidth is fixed and can be selected according to the applicable regional parameters (e.g., between 125, 250, and 500 kHz in the case of the EU 868 MHz band). These channels are specified in [8]. The European Telecommunications Standards Institute (ETSI) regulations allow using either a duty cycle (as required by LoRaWAN) or limitation, or to change the channel by using Listen Before Talk (LBT).

LoRaWAN Security

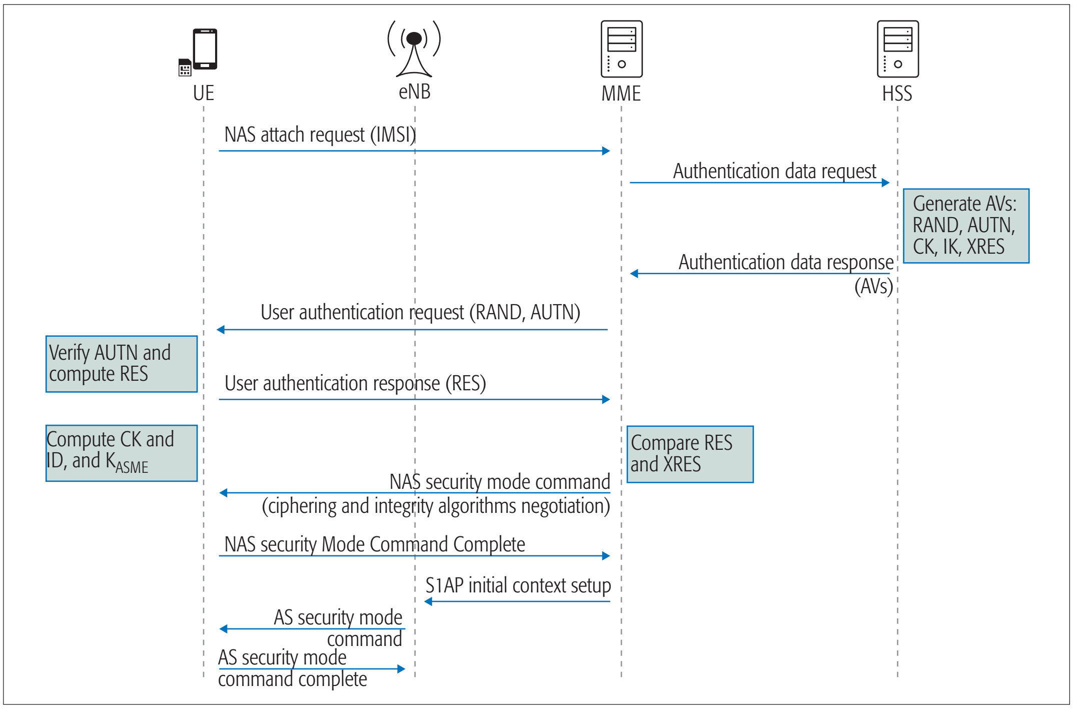
As previously mentioned, LoRaWAN is a technology with low power requirements intended for massive deployments. As security is crucial for the aforementioned applications, it has been included from the initial versions of the standard. Similar to the requirements for LoRaWAN communications, security is also designed for low power consumption, low implementation complexity, low cost, and high scalability [9].

The main properties of LoRaWAN security are mutual authentication, integrity protection, and confidentiality, which are summarized in Fig. 3.

As shown, an end device can be activated using either *over-the-air activation* (OTAA) or *activation by personalization* (ABP) [6]. Independent of whether OTAA or ABP is used, the device stores the following information: *DevAddr* (device address), *AppEUI* (application identifier), *NwkSKey* (network session key), and *AppSKey* (application session key). In the case of ABP, the device has to be previously customized with these parameters. In the case of OTAA, the device derives the session keys during the join procedure using the following information: *DevEUI* (a unique device identifier), *AppEUI* (an application identifier), and *AppKey* (an AES-128 key). When the activation is over the air, both the join request and accept messages include a message integrity code (MIC) computed using the Cipher-Based Message Authentication Code (AES-CMAC) algorithm with the *AppKey*, which allows each end to verify that the other end knows this key, thus achieving mutual authentication.

For data messages, integrity is achieved by also adding an MIC code. The MIC is computed using the AESCMAC algorithm with the *NwkSKey* over all the fields in the message. Then the MIC field is used by both the device and the network server to verify data integrity.

LTE security is based on the authentication and key agreement procedure, which allows both the UE and the eNB to achieve mutual authentication and to generate session ciphering (CK) and integrity (IK) keys. Different AKA procedures are implemented in the LTE security architecture to support UE access to the EPC via non-LTE access networks.



UE
eNB
MME
HSS
NAS attach request (IMSI)
Authentication data request
Generate AVs: RAND, AUTN, CK, IK, XRES
Authentication data response (AVs)
User authentication request (RAND, AUTN)
Verify AUTN and compute RES
User authentication response (RES)
Compute CK and ID, and K_{ASME}
Compare RES and XRES
NAS security mode command (ciphering and integrity algorithms negotiation)
NAS security Mode Command Complete
S1AP initial context setup
AS security mode command
AS security mode command complete

Figure 4. LTE security (EPS AKA).

Finally, end-to-end encryption is performed for application payloads exchanged between end devices and application servers. This means that the traffic is not only encrypted over the air interface, but it is also securely transported over the operator's core network. This approach eliminates the need for additional security layers, which may increase power consumption, complexity, and cost. The encryption scheme is based on AES with a key length of 128 bits (*NwkSKey*), allowing the encryption between the device and the network server.

LTE Security

LTE security [10] is based on the authentication and key agreement (AKA) procedure, which allows both the UE and the eNB to achieve mutual authentication and to generate session ciphering (CK) and integrity (IK) keys. Different AKA procedures are implemented in the LTE security architecture to support UE access to the EPC via non-LTE access networks.

As shown in Fig. 4, when a UE connects to the EPC over the evolved Universal Mobile Telecommunications System terrestrial radio access network (E-UTRAN), the AKA procedure is performed between the UE and the mobility management entity (MME). However, when a UE connects to the EPC via a non-3GPP access network [11], the authentication is done between the UE and an authentication, authorization, and accounting (AAA) server. If the UE has no preconfigured information, the non-3GPP access network is considered untrusted, and the UE needs to pass a trusted evolved packet data gateway (ePDG) connected to the EPC by establishing an IPsec tunnel using the Internet Key Exchange Protocol version 2 (IKEv2). If there is preconfigured information, the non-3GPP access network is considered trusted and the UE and the AAA server will utilize the Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) or Improved EAP-AKA (EAP-AKA').

LoRaWAN-EPC Secure Integration Proposal

As commented, mobile operators may be interested in deploying LPWAN networks in order to extend their market to massive IoT applications such as smart metering, remote monitoring, smart city applications, and asset tracking in the logistics industry.

Since MNOs have already deployed nationwide or even international WAN networks, including their O&M, it would be extremely beneficial to integrate IoT devices into their current mobile networks.

For that reason, we propose a novel and seamless integration of LoRaWAN with the 4G/5G core network (i.e., EPC). Our proposal provides the benefits of these two until now separate worlds. First, LoRaWAN end devices and servers are not modified, since the PHY and upper layers are kept untouched. As a result, the LoRaWAN security is maintained. More precisely, data integrity is ensured up to the network server, and data confidentiality is ensured up to the application server.

Second, the LoRaWAN gateway acts as a combination of UE and eNB for signaling with the EPC. It includes S1 setup for the connectivity between the eNB and the MME, and the attach and default bearer establishment.

For the latter control procedure, the LoRaWAN gateway is seen as an eNB from the EPC point of view, but it also includes the computation — typically done by the UE — of the required security parameters (e.g., the response parameter *RES* is calculated by the Universal Subscriber Identity Module, USIM, with the 128-bit random value

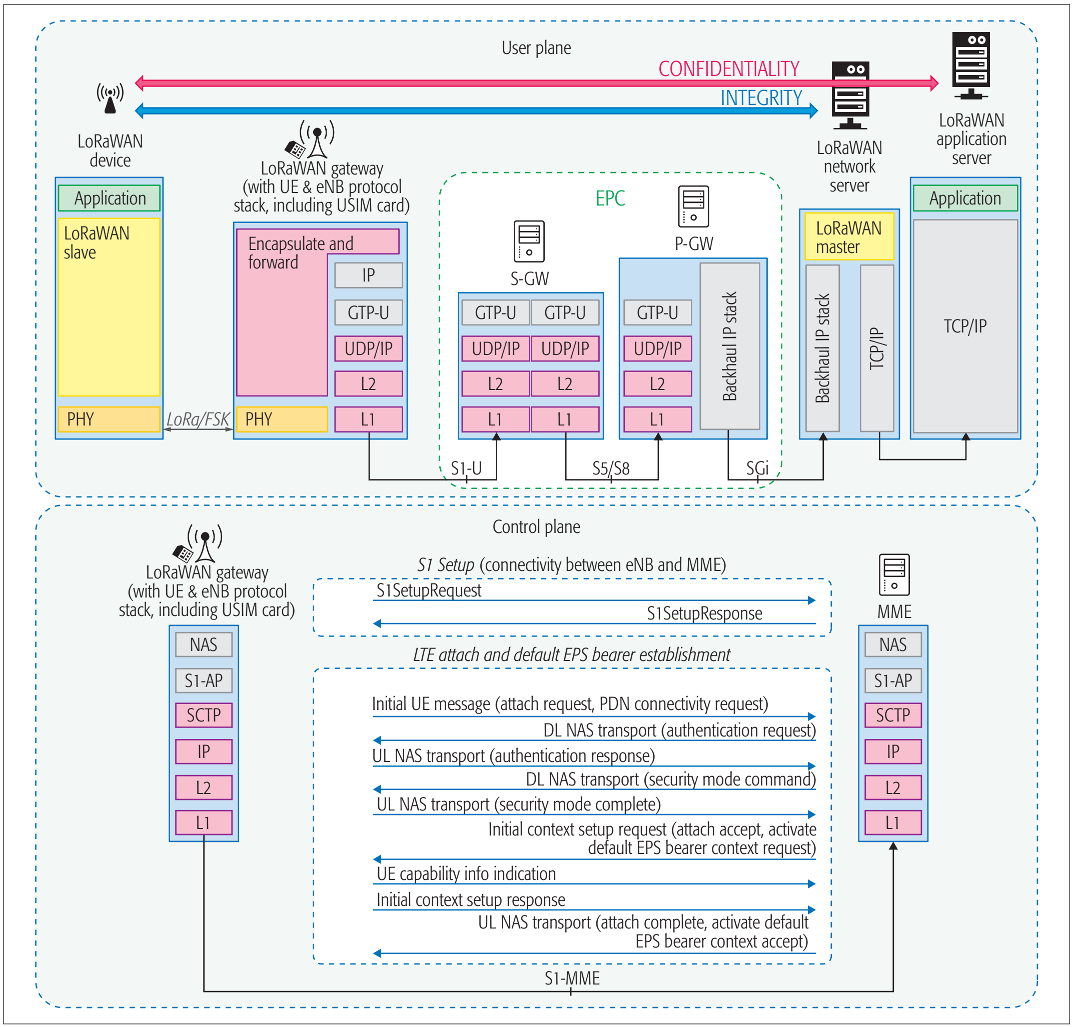

User plane
CONFIDENTIALITY
INTEGRITY
LoRaWAN device
LoRaWAN gateway (with UE & eNB protocol stack, including USIM card)
LoRaWAN network server
LoRaWAN application server
Application
LoRaWAN slave
PHY
LoRa/FSK
Encapsulate and forward
IP
GTP-U
UDP/IP
L2
L1
EPC
S-GW
P-GW
GTP-U
UDP/IP
L2
L1
Backhaul IP stack
LoRaWAN master
Backhaul IP stack
TCP/IP
Application
TCP/IP
S1-U
S5/S8
SGi
Control plane
LoRaWAN gateway (with UE & eNB protocol stack, including USIM card)
MME
NAS
S1-AP
SCTP
IP
L2
L1
S1 Setup (connectivity between eNB and MME)
S1SetupRequest
S1SetupResponse
LTE attach and default EPS bearer establishment
Initial UE message (attach request, PDN connectivity request)
DL NAS transport (authentication request)
UL NAS transport (authentication response)
DL NAS transport (security mode command)
UL NAS transport (security mode complete)
Initial context setup request (attach accept, activate default EPS bearer context request)
UE capability info indication
Initial context setup response
UL NAS transport (attach complete, activate default EPS bearer context accept)
S1-MME

Figure 5. LoRaWAN integration with a 4G/5G mobile network, both user and control planes, including the signaling between the LoRaWAN gateway and the EPC.

Our proposal only requires the modification of LoRaWAN gateways, which maintains their LoRaWAN protocols from the end-device perspective, but now includes the eNB protocols from the EPC point of view for both control and user planes.

RAND sent by the EPC). Thus, there is only one LTE bearer between the gateway and the EPC. This bearer is used to send all the data from/to the LoRaWAN end devices that are camping under the gateway coverage area.

Although it would be possible to establish one bearer per end device, due to their low data rates, it is not strictly necessary, but simplifies and reduces the signaling.

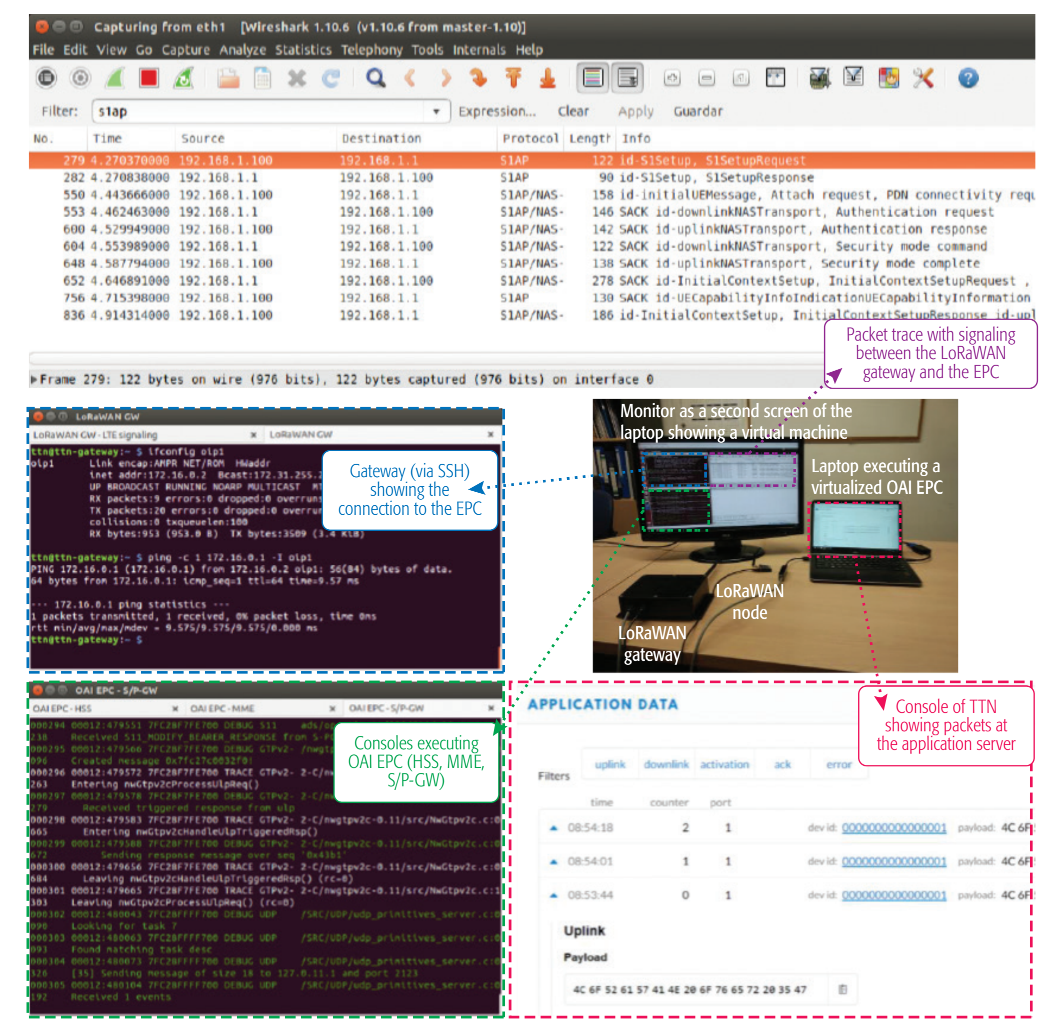
The proposed scheme is summarized in Fig. 5, including the main entities, user and control planes, protocol stacks, signaling messages, and interfaces. As shown, LoRaWAN devices and servers maintain their original protocols and signaling procedures. The EPC is also not modified, so the 4G/5G security procedures are unaffected. As an example, Fig. 5 also includes the EPS AKA case in the control plane, but alternatively it would be straightforward to use IKEv2 with the EAP-AKA (i.e., treating the gateway like an untrusted access network connected to the EPC). Our proposal only requires the modification of LoRaWAN gateways, which maintains their LoRaWAN protocols from the end-device perspective, but now includes the eNB protocols from the EPC point of view for both control and user planes.

Thus, both the end devices and the EPC are not modified, therefore achieving a seamless integration of LoRaWAN and 4G/5G technologies. Additionally, the end-to-end security is ensured thanks to the LoRaWAN integrity and confidentiality up to the network and application servers, respectively. It shall be noticed that these two entities, the network and the application servers, may or may not be part of the mobile operator infrastructure.

Additionally, we propose to leverage the USIM cards to improve the security of the LoRaWAN communications. In the case of ABP, the LoRaWAN device must store the 128-bit session keys *NwkSKey* and *AppSKey*. In the case of OTAA, the device must store the *AppKey*, which is used to derive the aforementioned session keys. In both cases, the security of the communications is compromised if a malicious user is able to get physical access to the device. For that reason, the usage of a cryptographic chip is highly beneficial. In the case of OTAA, these session keys can be computed using smart cards (e.g., Java cards), which can store the *AppKey* securely.

However, in order to leverage existing USIM cards, which are cheap and available to mobile operators, we propose to use the 128-bit ciphering and integrity keys *CK* and *IK* as the LoRaWAN session keys. These keys are derived

Since the gateway is connected to the LoRaWAN network server via the EPC, data traffic through the mobile core network is both integrity protected and encrypted. This can be easily checked using The Things Network console, which shows the encrypted data on the network server and the plain text data on the application server.



```
Capturing from eth1   [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
Filter: s1ap
No.  Time         Source         Destination    Protocol  Length Info
 279 4.270370000 192.168.1.100  192.168.1.1    S1AP       122 id-S1Setup, S1SetupRequest
 282 4.270838000 192.168.1.1    192.168.1.100  S1AP        90 id-S1Setup, S1SetupResponse
 550 4.443666000 192.168.1.100  192.168.1.1    S1AP/NAS-  158 id-initialUEMessage, Attach request, PDN connectivity requ
 553 4.462463000 192.168.1.1    192.168.1.100  S1AP/NAS-  146 SACK id-downlinkNASTransport, Authentication request
 600 4.529949000 192.168.1.100  192.168.1.1    S1AP/NAS-  142 SACK id-uplinkNASTransport, Authentication response
 604 4.553989000 192.168.1.1    192.168.1.100  S1AP/NAS-  122 SACK id-downlinkNASTransport, Security mode command
 648 4.587794000 192.168.1.100  192.168.1.1    S1AP/NAS-  138 SACK id-uplinkNASTransport, Security mode complete
 652 4.646891000 192.168.1.1    192.168.1.100  S1AP/NAS-  278 SACK id-InitialContextSetup, InitialContextSetupRequest ,
 756 4.715398000 192.168.1.100  192.168.1.1    S1AP       130 SACK id-UECapabilityInfoIndicationUECapabilityInformation
 836 4.914314000 192.168.1.100  192.168.1.1    S1AP/NAS-  186 id-InitialContextSetup, InitialContextSetupResponse id-upl
▸Frame 279: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Guardar

Packet trace with signaling between the LoRaWAN gateway and the EPC

```
ttn@ttn-gateway:~ $ ifconfig olp1
olp1      Link encap:AMPR NET/ROM  HWaddr
          inet addr:172.16.0.2  Bcast:172.31.255.2
          UP BROADCAST RUNNING NOARP MULTICAST  MT
          RX packets:9 errors:0 dropped:0 overruns
          TX packets:20 errors:0 dropped:0 overrun
          collisions:0 txqueuelen:100
          RX bytes:953 (953.0 B)  TX bytes:3509 (3.4 KiB)

ttn@ttn-gateway:~ $ ping -c 1 172.16.0.1 -I olp1
PING 172.16.0.1 (172.16.0.1) from 172.16.0.2 olp1: 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=9.57 ms

--- 172.16.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 9.575/9.575/9.575/0.000 ms
ttn@ttn-gateway:~ $
```

Gateway (via SSH) showing the connection to the EPC

Monitor as a second screen of the laptop showing a virtual machine

Laptop executing a virtualized OAI EPC

```
000294 00012:479551 7FC28F7FE700 DEBUG S11     ads/op
238    Received S11_MODIFY_BEARER_RESPONSE from S-P
000295 00012:479566 7FC28F7FE700 DEBUG GTPv2- /nwgt
096    Created message 0x7fc27c0032f0!
000296 00012:479572 7FC28F7FE700 TRACE GTPv2- 2-C/n
263    Entering nwGtpv2cProcessUlpReq()
000297 00012:479578 7FC28F7FE700 DEBUG GTPv2- 2-C/n
279      Received triggered response from ulp
000298 00012:479583 7FC28F7FE700 TRACE GTPv2- 2-C/nwgtpv2c-0.11/src/NwGtpv2c.c:0
665      Entering nwGtpv2cHandleUlpTriggeredRsp()
000299 00012:479588 7FC28F7FE700 DEBUG GTPv2- 2-C/nwgtpv2c-0.11/src/NwGtpv2c.c:0
672          Sending response message over seq '0x43b1'
000300 00012:479656 7FC28F7FE700 TRACE GTPv2- 2-C/nwgtpv2c-0.11/src/NwGtpv2c.c:0
684      Leaving nwGtpv2cHandleUlpTriggeredRsp() (rc=0)
000301 00012:479665 7FC28F7FE700 TRACE GTPv2- 2-C/nwgtpv2c-0.11/src/NwGtpv2c.c:1
303    Leaving nwGtpv2cProcessUlpReq() (rc=0)
000302 00012:480043 7FC28FFFF700 DEBUG UDP    /SRC/UDP/udp_primitives_server.c:0
090    Looking for task 7
000303 00012:480063 7FC28FFFF700 DEBUG UDP    /SRC/UDP/udp_primitives_server.c:0
093    Found matching task desc
000304 00012:480073 7FC28FFFF700 DEBUG UDP    /SRC/UDP/udp_primitives_server.c:0
326    [35] Sending message of size 18 to 127.0.11.1 and port 2123
000305 00012:480104 7FC28FFFF700 DEBUG UDP    /SRC/UDP/udp_primitives_server.c:0
192    Received 1 events
```

Consoles executing OAI EPC (HSS, MME, S/P-GW)

APPLICATION DATA

time	counter	port		
▲ 08:54:18	2	1	dev id: 0000000000000001	payload: 4C 6F
▲ 08:54:01	1	1	dev id: 0000000000000001	payload: 4C 6F
▲ 08:53:44	0	1	dev id: 0000000000000001	payload: 4C 6F

Uplink

Payload

4C 6F 52 61 57 41 4E 20 6F 76 65 72 20 35 47

Console of TTN showing packets at the application server

Figure 6. Testbed including the LoRaWAN gateway and the virtualized OAI EPC.

from the *RAND* value (sent by the network), the secret key *K* (stored in the USIM), and an operator-dependent value *OP*, using the *f3* and *f4* functions.

For USIM cards implementing the MILENAGE algorithm [12], *f3* and *f4* functions are based on AES-128 encryption (plus bitwise operations such as rotations and XOR functions). In the case of LoRaWAN devices using USIM cards as cryptographic chips, the input *RAND* value may be computed as a concatenation of *DevNonce*, *AppNonce*, and other parameters (e.g., *DevEUI* and NetId).

Proof of Concept

As a proof of concept, we implemented the proposed integration scheme in an experimental testbed. This testbed is part of the demonstrator developed in the 5GCity project, a coordinated research project that involves four Spanish universities and one non-profit research center.

The LoRaWAN gateway is based on a Raspberry Pi3 and an IMST iC880A LoRaWAN concentrator for the industrial, scientific, and medical (ISM) 868 MHz band. It is directly connected to an EPC, which is implemented using the *openair-cn* package of OpenAirInterface5G (OAI) [13]. All the EPC entities are virtualized and executed in one laptop with an Intel i7-4500U processor and 8 GB of DDR3 RAM. The host operating system (OS) is the 64-bit version of MS Windows 10 Enterprise (version 1607, build 14393-1593) executing VirtualBox 5.1.18, whereas the guest OSs are Ubuntu 16.04 LTS (64-bit). The gateway implements part of the eNB protocol stack based on code from OpenAirInterface5G, directly asking a USIM for the authentication parameters. For that purpose, the USIM is introduced in a smart card reader and queried using the *osmo-sim-auth* script [14].

Our LoRaWAN gateway is configured to connect to The Things Network (TTN) [15] back-end through the virtualized EPC. This back-end comprises different routing service components including the network and the application servers. For testing, we utilize a LoRa device based on Semtech's SX1176 and an Arduino-compatible microcontroller unit (MCU). Figure 6 shows our testbed in operation.

Since the gateway is connected to the LoRaWAN network server via the EPC, data traffic through the mobile core network is both integrity protected and encrypted. This can be checked easily using the TTN console, which shows the encrypted data on the network server and the plain text data on the application

[3] Figure 6 shows the TTN console with packets received by the application server. The payload is shown in plaintext, where the hex values 4c6C6F526157414E and 206F766572203547 are the ASCII codes for LoRaWAN over 5G.

server.[3] Hence, the LoRaWAN security is maintained in our solution, achieving end-to-end confidentiality.

Conclusions

Current forecasts predict several billions of IIoT devices by 2020, accounting for 57 percent of the overall IoT spending that year. Many of the IIoT use cases will generate mMTC traffic with low power, long range, and low bandwidth requirements. However, 3GPP cellular proposals for mMTC such as LTE-M and NB-IoT are not yet widely deployed due to their late standardization, and many mobile operators have started to employ LPWAN technologies such as LoRaWAN.

For this reason, in this article, we have presented a proposal for seamless integration of LoRaWAN and 4G/5G mobile networks. This solution is transparent to the LoRaWAN end devices and mobile network entities, which do not require any modification. Only the LoRaWAN gateway is modified, which is seen as an eNB from the EPC perspective, and implements the LTE signaling for S1 setup and the attach and default bearer establishment procedures. All data packets are sent through the EPC using only one LTE bearer to simplify and reduce signaling. End-to-end security is ensured thanks to the LoRaWAN procedures for integrity and confidentiality.

As a proof of concept, we implemented the proposed solution in an experimental testbed. For that purpose, we modified a LoRaWAN gateway to implement the required LTE signaling. The gateway was connected to a LoRaWAN network and application servers via a 4G/5G core network. These servers were part of The Things Network, whereas the core network was an unmodified OpenAirInterface EPC. Using our testbed, LoRaWAN end devices were able to send data to the application server while maintaining end-to-end security (in both integrity and confidentiality).

In the future, we will work on the design of a multi-tenant solution based on network slicing to share different radio access technologies, including 4G/5G and LoRaWAN, between multiple MNOs. Additionally, we will also work on the modification of the medium access control layer in order to improve the performance and the capacity of current LoRaWAN networks.

In the future, we will work on the design of a multi-tenant solution based on network slicing to share different radio access technologies, including 4G/5G and LoRaWAN, between multiple MNOs. Additionally, we will also work on the modification of the MAC layer in order to improve the performance and the capacity of current LoRaWAN networks.

Acknowledgments

This work is supported by the Spanish Ministry of Economy and Competitiveness and the European Regional Development Fund (projects TEC2016-76795-C6-4-R and UNGR15-CE-3311).

References

[1] A. Nordrum, "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated," *IEEE Spectrum*'s general technology blog, Aug. 2016; http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated, accessed Aug. 28, 2017, .

[2] P. Middleton *et al.*, "Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2016," Gartner Report, Dec. 2016; https://www.gartner.com/doc/3558917/forecast-internet-things–endpoints, accessed Aug. 28, 2017,

[3] R. Minerva, A. Biru, and D. Rotondi, "Towards A Definition of the Internet of Things rev. 1," *IEEE Internet of Things*, May 2015; http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf, accessed Aug. 28, 2017.

[4] SNS Research, "The LPWA Networks Ecosystem: 2017–2030 — Opportunities, Challenges, Strategies, Industry Verticals & Forecasts," Report, Nov.2016; http://www.snsintel.com/the-lpwa-low-power-wide-area-networks-ecosystem-2017-2030.html, accessed Aug. 28, 2017.

[5] R. Burbidge, "LTE-WLAN Aggregation (LWA) and LTE WLAN Radio Level Integration with IPsec Tunnel (LWIP)," doc. IEEE 802.11-16/351r1, presentation, Mar. 2016; http://www.3gpp.org/images/PDF/2016_03_LWA_LWIP_3GPPpresentation.pdf, accessed Aug. 28, 2017.

[6] N. Sornin *et al.*, "LoRaWAN Specification v1.0.2," LoRa Alliance Standard specification, July 2016; https://www.lora-alliance.org/lorawan-for-developers, accessed Aug. 28, 2017.

[7] Semtech, "AN1200.22, LoRa Modulation Basics," Application Note, May 2015; http://www.semtech.com/images/datasheet/an1200.22.pdf, accessed Aug. 28, 2017, .

[8] LoRa Alliance Technical Committee, "LoRaWAN Regional Parameters v1.0.2," LoRa Alliance Standards Spec., Feb. 2017; https://www.lora-alliance.org/lorawan-for-developers, accessed Aug. 28, 2017, .

[9] LoRa Alliance (Gemalto, Actility, and Semtech), "LoRaWAN Security, Full End-to-End Encryption for IoT Application Providers," White Paper, Feb. 2017; https://docs.wixstatic.com/ugd/eccc1a_cc44304714c14f80a6ce50fcf9fcee2a.pdf, accessed Aug. 28, 2017.

[10] 3GPP Tech. Spec. Group Service and System Aspects, 3GPP System Architecture Evolution (SAE); Security Architecture (Rel-15), 3GPP TS 33.401 V15.0.0, June 2017.

[11] 3GPPTech. Spec. Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security Aspects of Non-3GPP Accesses (Rel-14), 3GPP TS 33.402 V14.2.0, June 2017.

[12] 3GPP Tech. Spec. Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General (Rel 14), 3GPP TS 35.205 V14.0.0, Mar. 2017.

[13] OpenAirInterface 5G Wireless Implementation; https://gitlab.eurecom.fr/oai/openairinterface5g/, accessed Aug. 28, 2017.

[14] Osmo-sim-auth project; https://osmocom.org/projects/osmo-sim-auth/wiki, accessed Aug. 28, 2017.

[15] The Things Network; https://www.thethingsnetwork.org, accessed Aug. 28, 2017.

Biographies

Jorge Navarro-Ortiz (jorgenavarro@ugr.es) is an associate professor in the Department of Signal Theory, Telematics and Communications of the University of Granada, Spain. He obtained his M.Sc.E.E. from the University of Malaga, Spain, in 2001. Afterward, he worked at Nokia Networks, Optimi/Ericsson, and Siemens. He started working as an assistant professor at the University of Granada in 2006, where he got his Ph.D. His research interests include wireless technologies for IoT such as LoRaWAN and 5G.

Sandra Sendra [M] (ssendra@ugr.es) has a Ph.D. in electronic engineering. She is an assistant professor at the University of Granada. She has more than 100 scientific papers in international conferences, journals, and books. She is Editor-in-Chief of *WSEAS Transactions on Communications*, and a Guest Editor of Special Issues and Associate Editor fpr several international journals. She has been involved in more than 140 committees of international conferences through 2017. She has participated in 16 research projects.

Pablo Ameigeiras (pameigeiras@ugr.es) received his M.Sc.E.E. degree in 1999 from the University of Malaga. In 2000 he joined the Cellular System group at Aalborg University, Denmark, where he carried out his Ph.D. thesis. Afterward, he worked at Optimi/Ericsson. In 2006 he joined the University of Granada, where he has led several projects related to 4G/5G systems. His research interests include software defined networking and network functions virtualization for 5G systems.

Juan M. Lopez-Soler (juanma@ugr.es) is a professor in the Department of Signal Theory, Telematics and Communications, University of Granada. In 1991–1992 he joined the Institute for Systems Research at the University of Maryland. He is the head of the WiMuNet Lab at the University of Granada. He has participated in 24 research projects, has advised five Ph.D. theses, and has published more than 70 journal/conference papers. His research interests include middleware, multimedia communications, and 5G networking.