Comparison and Analysis of Security Aspects of LoRaWAN and NB-IoT

Authors:
Philipp Hofmann, Yvonne Schmitz, Bernd Quink, Mona Parsa, Jens Olejak

LIFE IS FOR SHARING.

Deutsche Telekom IoT
connect. digitize. get ahead.

Table of Contents

I. Abbreviations

3GPP ..... 3rd Generation Partnership Project
64QAM ..... 64-Symbols Quadrature Amplitude Modulation
AES ..... Advanced Encryption Standard
AKA ..... Authentication and Key Agreement
App ..... Application
AppSKey ..... Application Session Key
AS ..... Access Stratum
ASME ..... Access Security Management Entity
AV ..... Authentication Vector
BEST ..... Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices
CIoT ..... Cellular IoT
C-SGN ..... CIoT Serving Gateway Node
CRC ..... Cyclic Redundancy Check
CSS ..... Chirp Spread Spectrum
DTLS ..... Datagram Transport Layer Security
GSM ..... Global System for Mobile Communications
EEA ..... EPS Encryption Algorithm
EIA ..... EPS Integrity Algorithm
eNB ..... Evolved Node B
EPC ..... Evolved Packet Core
EPS ..... Evolved Packet System
EUI ..... Extended Unique Identifier
FNwkSIntKey ..... Forwarding Network Session Integrity Key
HS ..... Home Subscriber Server
IMSI ..... International Mobile Subscriber Identity
ISM ..... Industrial, Scientific and Medical
JSEncKey ..... Join Server Encryption Key
JSIntKey ..... Join Server Integrity Key
LoRa ..... Long Range
LoRaWAN ..... Long Range Wide Area Network
LPWA ..... Low Power Wide Area
LTE ..... Long Term Evolution
MAC ..... Message Authentication Code
MHz ..... Megahertz
MME ..... Mobility Management Entity
MNO ..... Mobile Network Operator
NAS ..... Non-Access Stratum
Nwk ..... Network
NwkSEncKey ..... Network Session Encryption Key
NwkSKey ..... Network Session Key
OFDM ..... Orthogonal Frequency Division Multiplex
OSCORE ..... Object Security for Constrained RESTful Environments
PDCP ..... Packet Data Convergence Protocol
RF jamming ..... Radio Frequency jamming
RRC ..... Radio Resource Control
SNwkSIntKey ..... Serving Network Session Integrity Key
UE ..... User Equipment
UICC ..... Universal Integrated Circuit Card
UMTS ..... Universal Mobile Telecommunications System
UP ..... User plane
USIM ..... Universal Subscriber Identity Module
XOR ..... exclusive-OR operation

II. Management Summary

As the two most commonly used Low Power Wide Area (LPWA) technologies, NB-IoT and LoRaWAN provide energy-efficient, long-range mobile connectivity to smart devices such as smart meters, simple trackers and sensors for machines and containers. Since black-hat hackers increasingly show interest in the Internet of Things, this paper compares the security of NB-IoT and LoRaWAN.

LoRaWAN's most widely used architecture v1.0 consists of the end devices, the gateways they connect to wirelessly, a network server and an application server. The process of integrating new devices into a network is well-secured if the so-called Over-the-Air Activation method is used. There are only minor drawbacks, such as the use of a deprecated encryption operation mode.

Concerning data transmission, LoRaWAN 1.0 ensures integrity for whole messages but not between network server and application server. End-to-end encryption of frame payloads is provided as a standard. However, there is a flaw in this: the network server – only an intermediate point in application communication – gains possession of the app encryption key during the join process of the end devices. This flaw has been corrected by the new architecture v1.1 introduced in 2017. Many other security vulnerabilities have been closed through this update. But unfortunately, v1.1 is still hardly used today.

At the physical layer, LoRaWAN uses unlicensed frequency bands. This makes conducting radio frequency (RF) jamming easy. However, LoRaWAN uses the very robust LoRa modulation. LoRa relies on constantly changing frequency. This makes it very difficult for an adversary to even receive data of interest.

The most critical weakness of LoRaWAN is the end devices: for cost reasons, they usually have no secure element, a chip that stores cryptographic information such as secret keys in a secure way. Thus, an attacker could succeed in extracting secret keys or in flashing the device with compromised firmware.

NB-IoT is based on LTE as specified by the 3GPP international standardization organization. Hence, NB-IoT benefits from the carefully developed and tested LTE security features. These include mutual authentication of end device and network, known cryptographic algorithms such as AES and a secure key generation and exchange. The air interface of NB-IoT is encrypted at user and/or control plane. However, there is no end-to-end encryption by default. But operators can introduce a higher security level by using security tunnels, for instance, from the core network to the application server. Also, they can implement end-to-end encryption via the DTLS protocol or, in future, via the energy-efficient protocols such as BEST (3GPP standard), OSCORE (LWM2M), or proprietary solutions.

The 3GPP specification limits integrity protection to the control plane. Luckily, NB-IoT allows the transmission of small user data via the control plane, making it nevertheless resistant against manipulation. A major advantage is that NB-IoT SIM cards are tamper-proof: they contain a secure element. Extracting key material is thus very difficult and unlikely in most cases.

A risk in cellular mobile networks is that an attacker could force an end device to use the less secure 2G mobile standard by pretending that no LTE is available. Additional security measures such as end-to-end encryption should be implemented for roaming in NB-IoT networks since several vulnerabilities in roaming have been discussed in the past. However, if an NB-IoT use case exclusively takes place in the home network of the mobile network operator, no extra transmission security mechanisms are required, since a high security level is already provided by default.

As a conclusion, while both LPWA technologies provide strong security, NB-IoT outperforms LoRaWAN in a highly critical aspect: the secure storage of the cryptographic keys. Using devices without a secure element significantly reduces the effectiveness of end-to-end encryption. Organizations using LoRaWAN are thus recommended to develop a security concept. This should prescribe end devices with a secure element, the secure OTAA join method and the latest LoRaWAN architecture v1.1. The security mechanisms of NB-IoT are based on the LTE radio standard. This ensures a high security level. Yet, encryption should always be used, and critical user data should be sent via the more secure control plane (data over NAS), as is already the default for most operators. Additional security should be considered for roaming.

1. Introduction

The Internet of Things (IoT) continues to grow. A considerable amount of use cases rely on low-cost IoT devices with long battery lifetimes. This is true for smart cities, predictive maintenance or smart metering, for instance. The second essential component of such use cases are mobile networks that transmit data energy-efficiently over long distances at acceptable costs: Low Power Wide Area (LPWA) networks.

The two most commonly used LPWA technologies today are NarrowBand IoT (NB-IoT) and Long Range Wide Area Network (LoRaWAN). NB-IoT is based on LTE and was standardized by the mobile standards organization 3rd Generation Partnership Project (3GPP) in 2016. Networks of this kind operate on licensed spectrum [1]. The amount of NB-IoT connections worldwide is assumed to be 130 million – and to reach 740 million in 2023. LoRaWAN, in contrast, is developed by the LoRa Alliance™, an open association of companies from different sectors such as telecommunications and system integration. The standard was first introduced in 2015 and defines the communication protocol and system architecture for a LPWA network. The technology relies on unlicensed spectrum. While today, in 2020, the number of LoRaWAN connections is approximately 191 million, it is estimated to grow to 731 million in 2023. [2] [3]

While more and more IoT use cases use NB-IoT or LoRaWAN technology, security specialists have observed IoT-related attacks increasing sharply for years. For instance, the Mirai botnet and its derivatives still account for a large amount of IoT malware attacks. Therefore, this whitepaper takes a look at the security of NB-IoT and LoRaWAN. The security of the technologies is first discussed separately. The paper concludes by directly comparing the security features of both LPWA technologies.

2. Essential encryption schemes

The following chapter describes important encryption schemes that are used in LoRaWAN and NB-IoT.

AES

LoRaWAN and NB-IoT both use the Advanced Encryption Standard (AES) in order to ensure confidentiality. AES is a widely used encryption method. The procedure was published in 1998 and certified in 2000. It is a symmetrical encryption method where both communication parties share a common secret key. Therefore, it should always be ensured that both parties receive the secret key in a secure way. Under the assumption of appropriate key lengths, AES is supposed computationally secure. This means that the encryption cannot be cracked in an acceptable time even with very high computing power.

The block size to be encrypted is always 128 bits with AES. Only the key length is variable. Common key lengths are 128, 192 or 256 bits. The larger the key length is, the more secure but also complex and energy-consuming the encryption is. However, even AES-128 is assumed computationally secure today. [4,5,6] In the future, however, the high computing power of quantum computers could lead to the need for longer AES keys.

It is important to understand that the security of AES also heavily depends on its mode of operation. The mode of operation defines how messages of more than 128 bits – thus consisting of more than one block – are encrypted. AES supports a variety of different modes, which have advantages and disadvantages. The most popular are discussed in the following [7]:

Electronic Code Book Mode (ECB):

In ECB mode, each block is encrypted separately and independently from each other. ECB is a deterministic ciphering mode: the encryption of the same message always yields the same cipher text. However, the design of ECB has one major drawback: it preserves message patterns. Therefore, the use of AES in ECB mode is not recommended.

Cipher Block Chaining Mode (CBC)

The CBC mode relies on a randomly chosen binary string, the so-called initialization vector. This string is combined with the first message block using an exclusive-OR operation (XOR) and is only encrypted afterwards. For each block that follows, the message is XORed with the preceding cipher text before being encrypted. Thanks to the random factor and the dependency between the different cipher blocks, CBC does not suffer from the same weakness as ECB. A disadvantage, however, is that errors could be propagated throughout the message. Furthermore, CBC is malleable. This means that an attacker could modify a cipher text so that the decrypted plaintext is still related to the original plaintext. For instance, if the adversary flips two bits in the ciphertext, the same bits would flip in the plaintext. CBC is also used in the CMAC message authentication code (MAC) scheme that protects a message against manipulation. CMAC is supposed secure since it is probably not possible for an adversary to forge a valid MAC without having the secret key.

Counter Mode (CTR)

Similar to CBC, in CTR mode a random binary string is chosen for every new message, in this case a counter. This counter is incremented and encrypted for each message block. The resulting pseudorandom string is finally XORed with the plaintext message. Hence, CTR in fact turns the AES block cipher into a stream cipher. While CTR also overcomes the ECB weakness, it suffers from malleability too. An additional advantage of CTR is its ability to speed up encryption and decryption by precomputing the pseudorandom string and parallelizing the XOR operations for the message blocks.

Counter with CBC-MAC (CCM)

The CCM mode combines CTR mode with a CBC-MAC that is quite similar to CMAC but not secure for messages of variable length. Hence, CCM is a combined encryption and authentication block cipher mode [7] [8].

Although AES is supposed a secure encryption scheme, its security level also depends on its implementation. Flaws in the implementation could still insert vulnerabilities in an actually secure cryptographic scheme. Hence, the use of AES only cannot lead to the conclusion that a system provides confidentiality in a secure way.

AES in LTE networks

In LTE networks, four encryption algorithms can be used for the control and user plane on the radio path: EEA0, EEA1, EEA2 and EEA3 [9] (see also 4.2.2). While EEA0 means no encryption at all, the other EEA methods define a symmetric synchronous stream cipher. This ensures a fast encryption since the cipher stream can be precomputed and XORed to the plain text bit by bit. EEA1 relies on SNOW 3G (see below), EEA3 on the Chinese algorithm ZUC. The 128-EEA2 algorithm is based on 128-bit AES encryption in CTR mode. However, the EEA2 specifications extend the AES CTR method with some additional rules. It is thus more complex than the original algorithm [10].

The same is true for the integrity algorithm 128-EIA2 that is used to protect control and user plane data from manipulation. Being one of four EIA options, EIA2 is based on the secure 128-bit AES CMAC method.

SNOW 3G

The LTE encryption algorithm 128-EEA1 as well as the integrity algorithm 128-EIA1 are based on the SNOW 3G cipher [9]. SNOW 3G [11] is a word-oriented stream cipher that was first introduced by the 3GPP in 2006 and has already been used in UMTS. The algorithm produces a pseudorandom sequence of 32-bit words. This is used to mask the plaintext.

BEST

The 3GPP is working on a special security protocol for devices with energy constraints that need to communicate with low throughput but high latency over LTE or 5G networks. This service is called Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST) [12]. The three most important instances within the BEST protocol are the user equipment, the security endpoint in the network of the service provider (HSE) and the enterprise's application server (EAS). BEST can be used in three modes:

- for key agreement only
- for integrity protection
- for integrity and confidentiality protection

The integrity protection algorithm and the length of the MAC are selected by the HSE upon session start. The same is true for the encryption algorithm. The BEST standard relies on the same cryptographic mechanisms as LTE[1] . With BEST, the MAC for a message is calculated first and encrypted together with the payload to be protected afterwards. The cryptographic keys can be refreshed anytime during a session. The security features are provided for both user and control plane message. Control plane messages are terminated at the service provider. However, user plane messages can be protected between user equipment and service provider (end-to-middle), or between user equipment and application server (end-to-end).

BEST uses the approved LTE network elements for security purposes such as authentication (see 4.2.1) – adding another layer of security to LTE.

[1] In the BEST standard, only the EEA0 algorithm – meaning no encryption – is expected to be supported by the user equipment. However, in the Deutsche Telekom network using EEA0 is forbidden.

3. Security of LoRaWAN

LoRaWAN defines a system architecture for a LPWA network as well as a MAC protocol corresponding to layer 2 of the OSI model with some elements of layer 3 [3]. As an open specification defined by the LoRa Alliance, LoRaWAN can be used by telecom operators for public networks as well as by companies, other organizations or private persons for private networks. Especially in the latter case it is very important to ensure security of the LoRaWAN network to minimize security risks caused by ignorant or incautious users. The following sections describe the security implications of the LoRaWAN physical layer and of the two LoRaWAN architecture versions available today.

3.1. Modulation: LoRa and Chirp Spread Spectrum

LoRaWAN defines a system architecture for an LPWA network as well as a MAC protocol corresponding to layer 2 of the OSI model with some elements of layer 3 [3]. As a proprietary protocol developed by Semtech and supported by the LoRa Alliance, LoRaWAN is used by telecom operators for public networks as well as by companies, other organizations or private persons for private networks. Especially in the latter case it is very important to ensure security of the LoRaWAN network to minimize security risks caused by ignorant or incautious users. The following sections describe the security implications of the LoRaWAN physical layer and of the two LoRaWAN architecture versions available today.

Electronic Code Book Mode (ECB):
Before going deeper into the security aspects of LoRaWAN, it is important to distinguish LoRa (Long Range) from LoRaWAN, as the two concepts are often mistakenly considered to be the same thing. While LoRaWAN primarily describes the MAC layer of an LPWA network, LoRa is the modulation technology and thus part of the physical layer. LoRa is a special modulation developed by the French company Cycleo, which has been taken over by the chip manufacturer Semtech [13]. Consequently, the modulation is considered proprietary.

The second part of the physical layer is the regional ISM band, the carrier frequencies in each country. LoRa relies on sub-1-GHz carrier frequencies. In Europe, LoRaWAN can use the unlicensed carrier frequency bands of 433 MHz and 868 MHz. Figure 2 shows the different layers of the protocol stack.

The use of unlicensed frequencies has one problem: interference can easily occur, especially since anyone can use these frequencies. Furthermore, radio frequency (RF) jamming is easier in unlicensed spectrum than in licensed one. Therefore, LoRa is based on a very complex modulation method: chirp frequency spreading (CSS). CSS is a frequency spreading method and has been used since World War II; however, still today it is considered very robust and rather difficult to intercept. Chirp pulses are transmitted as symbols that continuously rise or fall in frequency over time. Data transmission is then realized by stringing these chirp pulses together in time. Due to the chirp pulses, CSS uses a large bandwidth.

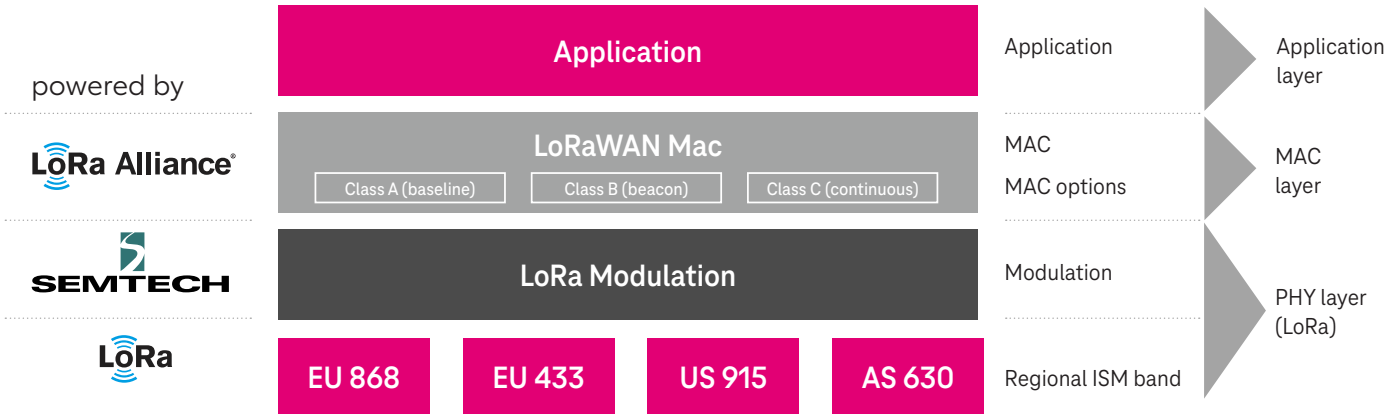


Figure 1: Layer structure and classification of LoRaWAN and LoRa [3]

One advantage of the CSS method is a great robustness against narrow-band interference and disturbances such as the Doppler effect. Furthermore, CSS provides a certain level of obscurity: as the frequency changes continuously, an eavesdropper may find it difficult to intercept complete messages. An adversary might even have problems detecting that a transmission is taking place at all. Figure 3 shows the continuous frequency change during the different fields of a LoRa frame. However, "security through obscurity" is not considered a reliable approach today and therefore does not eliminate the need for additional security measures on the upper layers. The disadvantages of the CSS modulation are a high complexity in signal reception and the need for large bandwidth at low transmission frequencies (see Table 1).

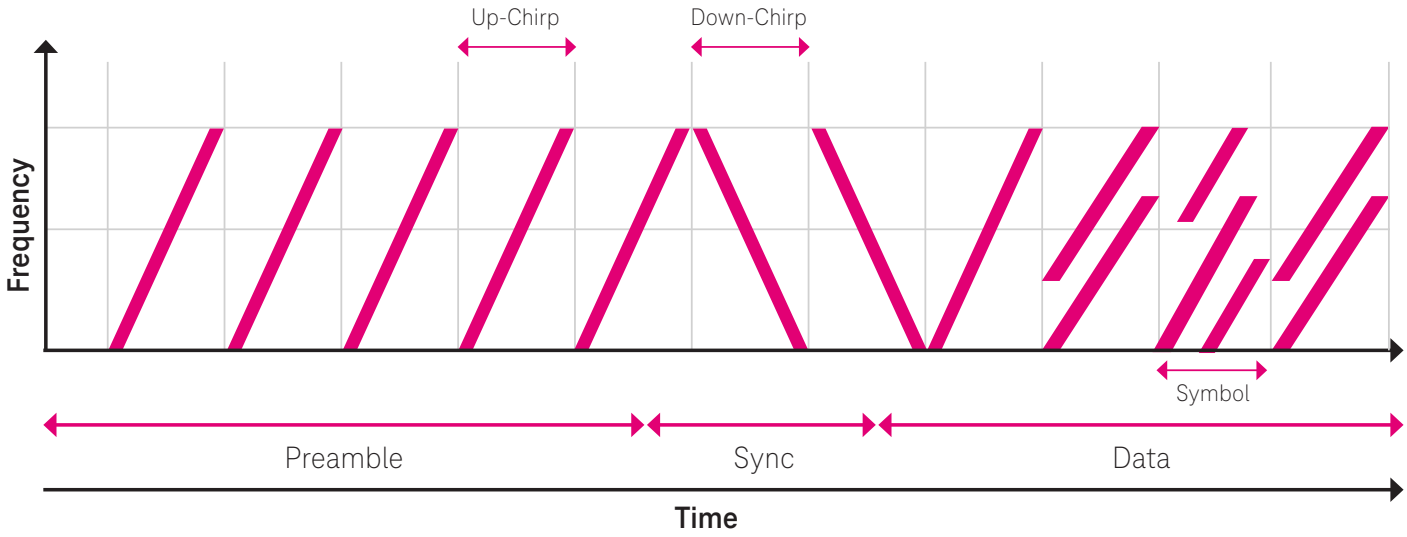


Figure 2: Chirp Spread Spectrum (CSS) modulation [14]

Advantages and disadvantages of CSS

Advantages:

- ⊕ **Great robustness** against disturbances and interferences
- ⊕ **Signal obscurity:** an adversary can not reliably eavesdrop on message content without authorization.

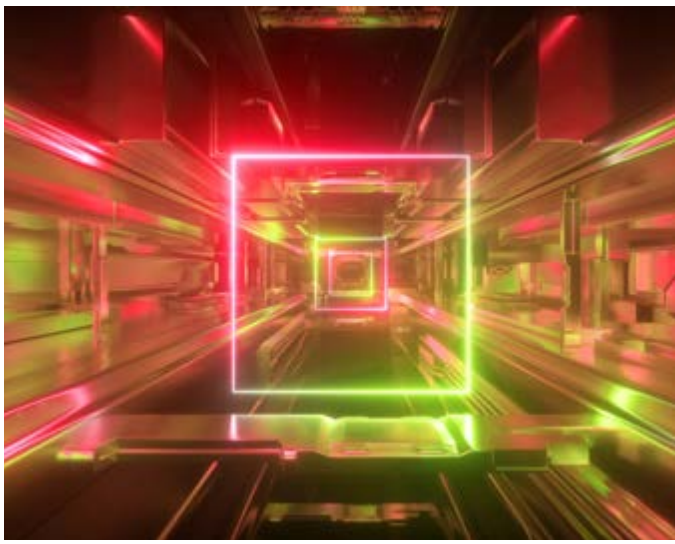
Disadvantages:

- ⊖ **RF jamming** is possible
- ⊖ **High complexity** at reception
- ⊖ **Large bandwidth**, required at lower transmission frequencies

Table 1: Advantages and disadvantages of Chirp Spread Spectrum

3.2. LoRaWAN architecture v1.0

The most common and most used LoRaWAN architecture today is v1.0. This version was first introduced in January 2015. LoRaWAN networks have a star topology (see Figure 5). They consist of the distributed LoRaWAN end devices; the gateways, network server and application servers. The end device does not care which gateway receives the data packets and transmits its packets to all gateways within reach. These in turn forward the messages to the cloud-based network server via some backhaul technology (e.g. Ethernet). The network server removes duplicates and forwards the packets to the appropriate application server. The application server executed the desired action. [3] Despite application data, LoRaWAN messages can be used to submit MAC commands between end device and network server for network administration purposes [15].



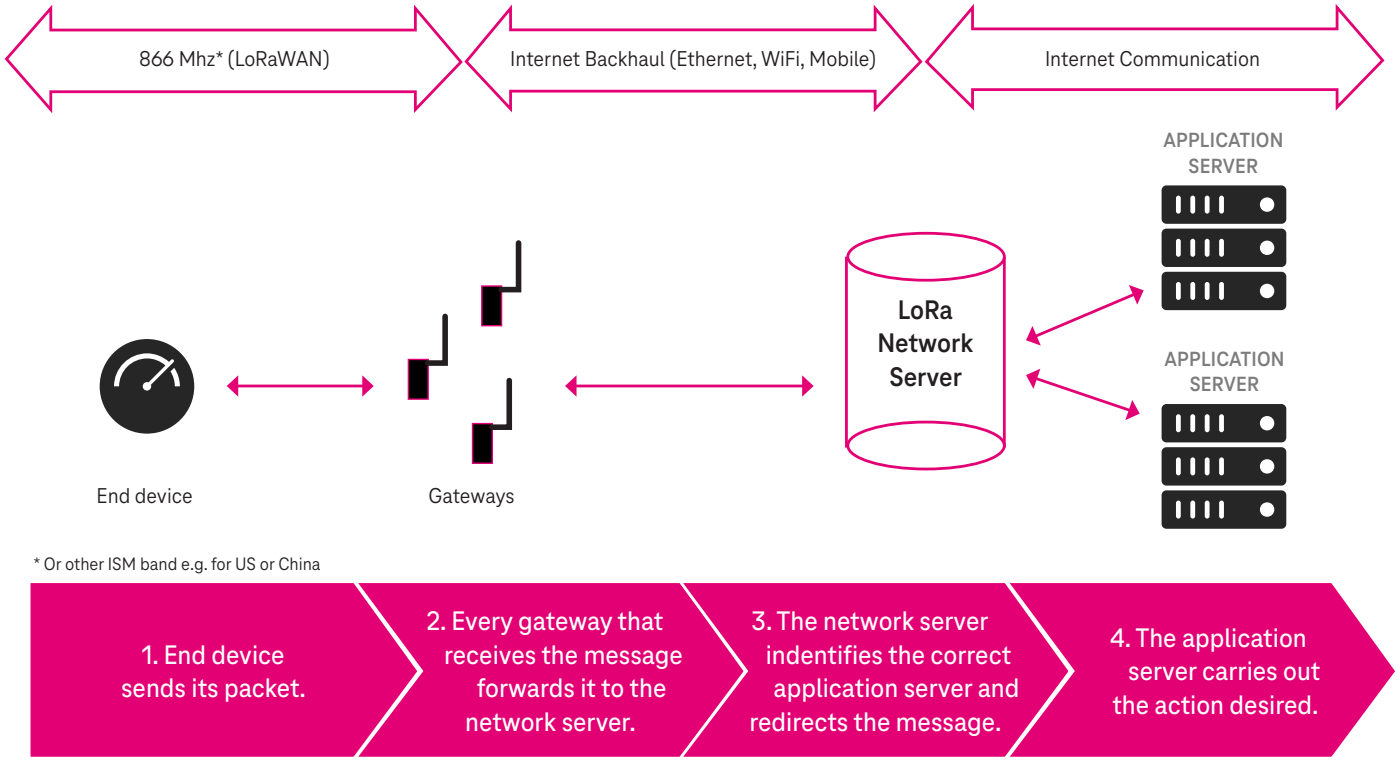


Figure 3: LoRaWAN v1.0 architecture [4]

3.2.1. Join process of LoRaWAN end devices

Identifiers and keys

In order to integrate end devices into a LoRaWAN v1.0 network (join process), several keys and identifiers are needed (see Table 2). A unique identification is guaranteed by the identifiers AppEUI and DevEUI. The DevEUI is assigned to the device by the device manufacturer. The AppEUI must be implemented in the device itself and is used to address the correct application server. The device also needs an address – the DevAddr – that is unique in the network.

With LoRaWAN v1.0, end devices only have one master key, the AppKey. This is key is pre-configured by the device manufacturer. To protect data transmissions, two session keys are needed: the NwkSKey that is mainly used for message authentication and the AppSKey for encryption [15].

Joining using Activation by Personalization (ABP)

Two join methods are available for LoRaWAN end devices. The simpler solution is called Activation by Personalization (ABP) (see Figure 6). However, ABP is only recommended for test devices since it has an essential security flaw: the two session keys used for message encryption and authentication are permanently implemented in the device. ABP does not support re-keying. Hence, message flows of an ABP-joined device – even from the past – are protected only as long as the session keys have not been compromised. ABP thus fails to provide perfect forward secrecy. Furthermore, network administrators could use insecure session keys or re-use keys for several devices, thus increasing the attack surface. [15]

Joining using Over-The-Air Activation (OTAA)

The join method recommended in terms of security is Over-The-Air Activation (OTAA). With OTAA, the device receives its unique device identifier (DevEUI) at manufacturing time – but the unique application ID (AppEUI) and the master key (AppKey) only at network registration. The join procedure consists of two messages between device and network server: the join-request and the join-accept message (see Figure 4).

First, the end device sends a join request to the network server containing the two identifiers AppEUI and DevEUI. Furthermore, a random nonce is sent to protect against replay attacks, where an adversary resends an earlier join-request. [15] However, research has shown that this mechanism is not sufficient: an end device could be prevented from connecting to the network by manipulating the random-number generator to reuse a nonce within a certain time [16]. The join-request is not encrypted but integrity-protected using AES-128-CMAC: the end device uses the pre-configured master key AppKey to calculate a MIC for the complete message. Thus, it also implicitly authenticates by demonstrating possession of the secret master key.

The network server validates the MIC using the AppKey stored for the device. It also checks the nonce against a limited list of nonces used by the end device in the past. Finally, the server sends a join-accept message to the end device, providing it with its device address (DevAddr), a network identifier (NetID) and another nonce. The whole message is first encrypted using an AES-128 decrypt operation in ECB mode. The choice of ECB mode, however, is somewhat strange since this operation mode is known to prevent patterns in encrypted data (as described in Chapter 2). The encrypted join-accept message is protected by a MIC calculated using the AppKey.

End device and network server now calculate the session keys NwkSKey and AppSKey. This is done by encrypting a string that contains the network identifier and the nonces using AES-128 and the AppKey [15]. However, using one master key to derive the secret keys for integrity and confidentiality protection is not recommended from a security perspective. The network server transmits the AppSKey to the application server after the join process is finished and is supposed to delete this session key afterwards [17]. If the mobile device loses the keys or the connection to the network, or if the network terminates the validity of the keys, the mobile device must initiate a new join procedure.

Conclusion

Anyone running or using LoRaWAN network should always use the OTAA method. This method is by far the most secure join method for LoRaWAN networks in standard operation. To clarify this again, the two login and authentication processes are compared in Table 2.

LoRaWAN v1.0				
Key	Description	Required in Joining Type		Generation
		OTAA	ABP	
Keys needed before activation				
AppKey	Is used to derive AppSKey and NwkSKey and to secure the OTAA join procedure.	Yes	No	Stored beforehand
Keys needed after activation				
NwkSKey	Is used to calculate/verify MICs and to encrypt MAC-only packets	Yes	Yes	ABP: manually generated OTAA: generated from AppKey and join-accept message
AppSKey	Is used to encrypt/decrypt payload of data packets	Yes	Yes	ABP: manually generated OTAA: generated from AppKey and join-accept message
Identifiers				
AppEUI	64-bit globally unique application ID	Yes	No	Stored beforehand
DevEUI	64-bit globally unique device ID assigned by the network server	Yes	No	Stored beforehand
DevAddr	32-bit unique device address in the current network	Yes	Yes	ABP: manually generated OTAA: received by join-accept message

Table 2: Security keys and identifiers in a LoRaWAN architecture v1.0 [15]

Figure 4: OTAA registration process of a LoRaWAN device [9]

Activation by Personalization (ABP)

Advantages:

- ⊕ **Simplified** commissioning process
- ⊕ **Fast:** Devices become immediately functional

Disadvantages:

- ⊖ **Manual generation of session keys** could lead to re-used or insecure keys.
- ⊖ **No re-keying** possible

Over-the-Air Activation (OTAA)

Advantages:

- ⊕ **Integrity and confidentiality protection** for join messages
- ⊕ **Implicit mutual authentication** by proving possession of master key
- ⊕ **Secure key generation** using AES-128, nonces and the master key
- ⊕ **Re-keying of session keys** is possible

Disadvantages:

- ⊖ **AES in the unrecommended ECB mode** is used for encryption
- ⊖ **Need for improved key generation** since master key is used for both session keys

Table 3: Advantages and disadvantages of the LoRaWAN v1.0 join methods

3.2.2. Data transmission

LoRaWAN frames consist of five fields as described in Table 4. Each message is integrity-protected by a MIC that is calculated over all fields of the MAC frame including headers and payload. Like with OTAA, AES-128-CMAC and the NwkSKey is used for MIC calculation. However, if the payload (FRMPayload) is not empty, the FRMPayload field must be encrypted before MIC calculation. The encryption scheme used is AES-128 in CCM* mode, an extension of the CCM mode. For encrypting application data, the AppSKey is selected. [15] [8]

Frames carrying MAC commands only are thus integrity- and confidentiality-protected end-to-end between end device and network server (see **Table 5**). Frames carrying application data are end-to-end encrypted between end device and application server. Yet, during the OTAA join process the network server is in possession of the AppSKey and would be able to decrypt application data if the key is not deleted as desired by the LoRaWAN specification. Furthermore, integrity is only ensured between end device and network server. Hence, application payloads might be manipulated by a network server or during transmission towards the application server. This is because in LoRaWAN specification v1.0 network services are considered as trusted parties. To close this security gap, LoRaWAN network operators should implement additional security measures such as a VPN between network server and application server. [15]

MHDR	FHDR
MAC header	Frame header
Integrity-protected	Integrity-protected
FPort	**FRMPayload**
Optional, specifies type of FRMPayload	Payload containing MAC commands and/or application data
Integrity-protected	Integrity-protected and encrypted
MIC	
Message integrity code	

Table 4: Frame format of LoRaWAN data message [15]

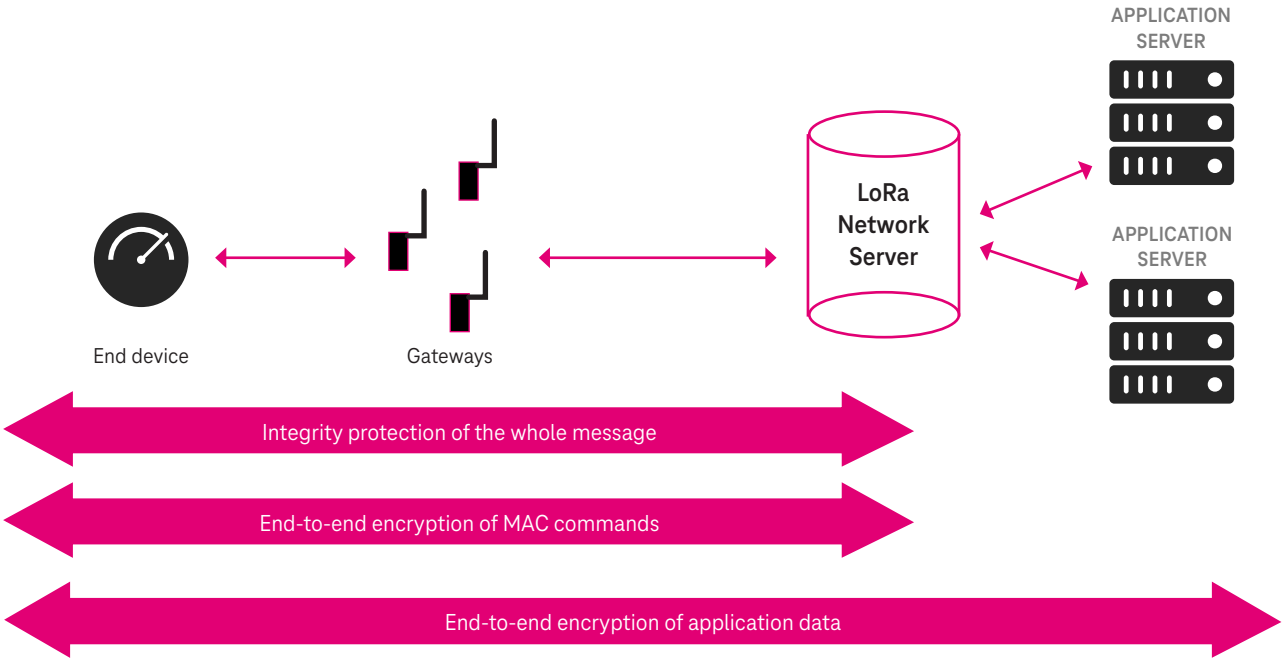


Figure 5: Security of LoRaWAN data messages

Advantages:

- ⊕ **Integrity protection** for all frame fields
- ⊕ **End-to-end encryption** for application data and MAC commands

Disadvantages:

- ⊖ **Integrity protection for application data** only between end device and network server
- ⊖ **Flaw in the end-to-end encryption** for application data since the network server has the encryption key

Table 5: Advantages and disadvantages of LoRaWAN v1.0 data transmission

Scientific research has shown that the LoRaWAN architecture v1.0 has several security vulnerabilities of varying degrees of severity. Some of these have already been mentioned in previous chapters. The following LoRaWAN v1.0 vulnerabilities are well known.

LoRaWAN endpoints contain a master key that does not change during their lifetime and may also be used for the entire network. Compromised keys will thus disclose past and current messages – potentially in the whole network. Furtermore, cost-efficiency is one of the most important criteria for these devices. Therefore LoRaWAN devices often have no secure element that stores cryptographic information in a secure way. Attackers, hence, could succeed in extracting keys from an end device they get their hands on or introduce malicious firmware. One limitation of the end-to-end encryption of application data is that the network server originally knows the session key AppSKey (as described in 3.2.1) [17]. It is not certain whether the AppSKey is securely deleted by the network server after the join process.

Most LoRaWAN end devices are only occasionally connected to the network. This fact can be used to perform physical hacks more easily without being noticed immediately. Another thing to be aware of is that LoRaWAN ensures no integrity between network and application server and uses the master key as a basis for both session keys. Finally, in case of a possible compromise, it can be very difficult to restore a secure state for a LoRaWAN network: the AppKey has to be changed for each device. With a lot of devices, this turns out to be very costly and complex.

These security vulnerabilities are used, among others, to execute certain attacks. Table 6 provides an overview of attacks that could be possible. The two attacks with the supposedly highest impact are physical gateway attacks and malicious gateway attacks. Both assume that an adversary gets access to one or more LoRaWAN gateways. In a physical gateway attack, the adversary could disable the gateways and thus cripple the network. In a malicious gateway attack, sensor data could be redirected to a malicious network server. In consequence, the attacker might try to manipulate messages. [18]

Attack	Costs	Expertise	Result	Detectability	Avoidability	Potential Impact
Counter Overflow Introducing messages with frame counter 0 to make valid messages being ignored (only with ABP)	low	high	fake messages	medium	easy	small
Physical Gateway Attack Disabling gateways to slow down or cripple the network	low	medium	cripple networks	easy	medium	high
Malicious Gateway Attack Manipulating gateways to redirect messages to a fake network server	medium	high	fake messages	difficult	medium	high
Physical Sensor Attack Eavesdropping sensor data from communication between two chips within an end device	medium	medium	fake messages	difficult	difficult	small
Generic Jamming Sending on the same frequencies to disturb the transmission of all packets	high	low	cripple networks	easy	difficult	small
Selective Jamming Sending on the same frequencies to disturb the transmission of a specific packet	high	high	fake messages	difficult	medium	small
Replay Attack Resending an originally sent message	low	high	fake messages	difficult	easy	small
Wormhole Attack Stopping a message from being received by a jamming attack and replaying the message afterwards	high	high	fake messages	difficult	medium	small

Table 6: Investigated attacks and their impact on a LoRaWAN architecture v1.0 [18]

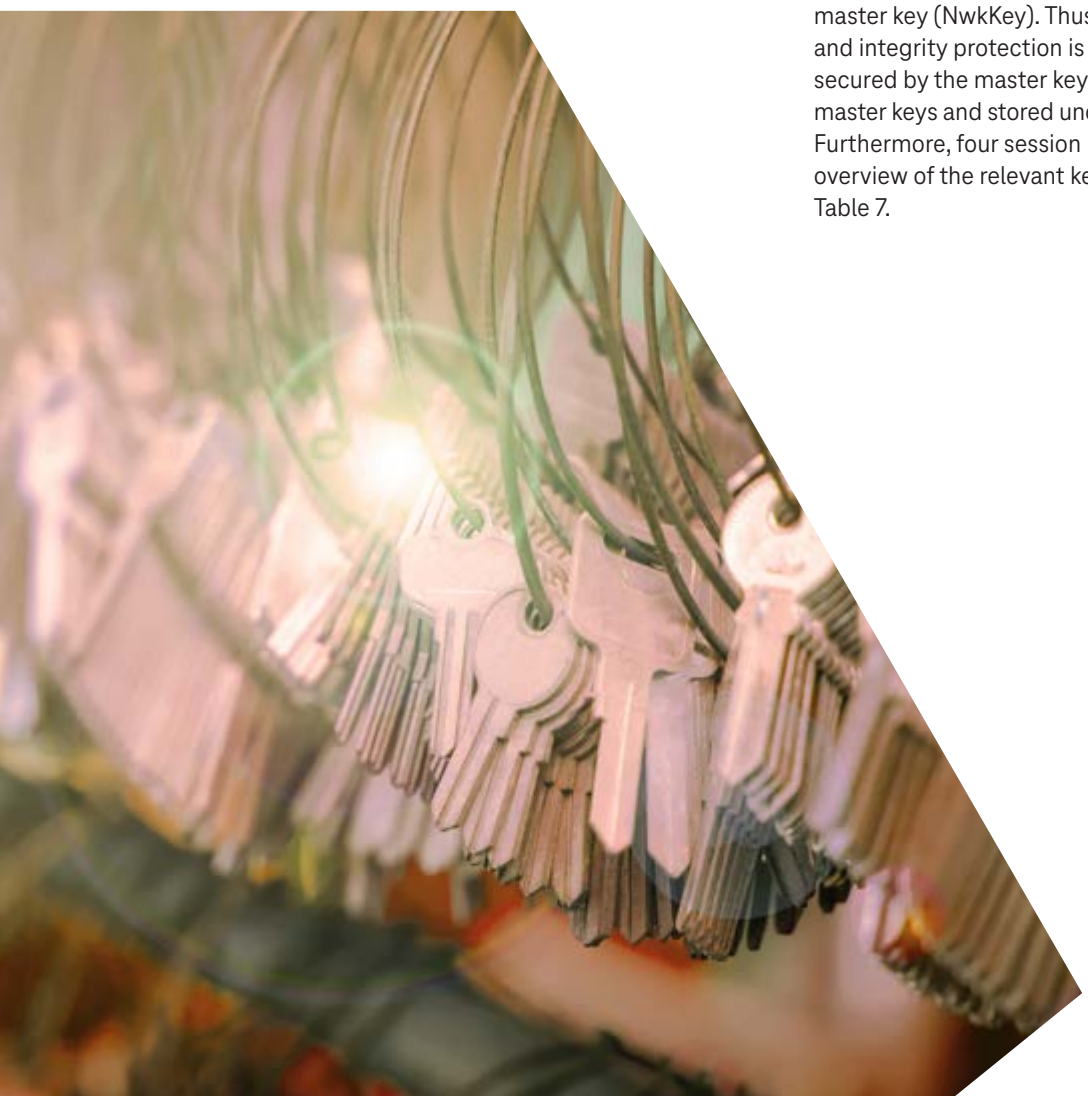
3.3. LoRaWAN architecture v1.1

The LoRa Alliance is also aware of the weaknesses mentioned in 3.2.3. This is why a new LoRaWAN architecture was launched in October 2017. As of today (September 2020), however, there is still no known provider who has rolled out the LoRaWAN v1.1 architecture on a large scale. However, some critical vulnerabilities have been closed with the new architecture, and it will probably be used more widely in the future. Hence, architecture v1.1 will be covered here as well.

The largest changes compared to LoRaWAN v1.0 are three servers that have been added to the architecture (see Figure 6):

- A join server: The join server takes over the management of the OTAA join process from the network server. It is responsible for generating the session keys. While the network session key is sent to the network server afterwards, it never gains possession of the AppSKey used for encrypting application data. Hence, real end-to-end encryption is realized on application level.
- Two additional network servers for serving and forwarding: These allow roaming packets to foreign LoRaWAN networks.

Another improvement is that the network session key is no longer generated from the AppKey but from a separate, pre-configured master key (NwkKey). Thus, a clear separation of confidentiality and integrity protection is guaranteed. The join process is not secured by the master key but two join keys generated from the master keys and stored unchanged for the device's whole lifetime. Furthermore, four session keys are used instead of two [19]. An overview of the relevant keys for LoRaWAN v1.1 can be found in Table 7.



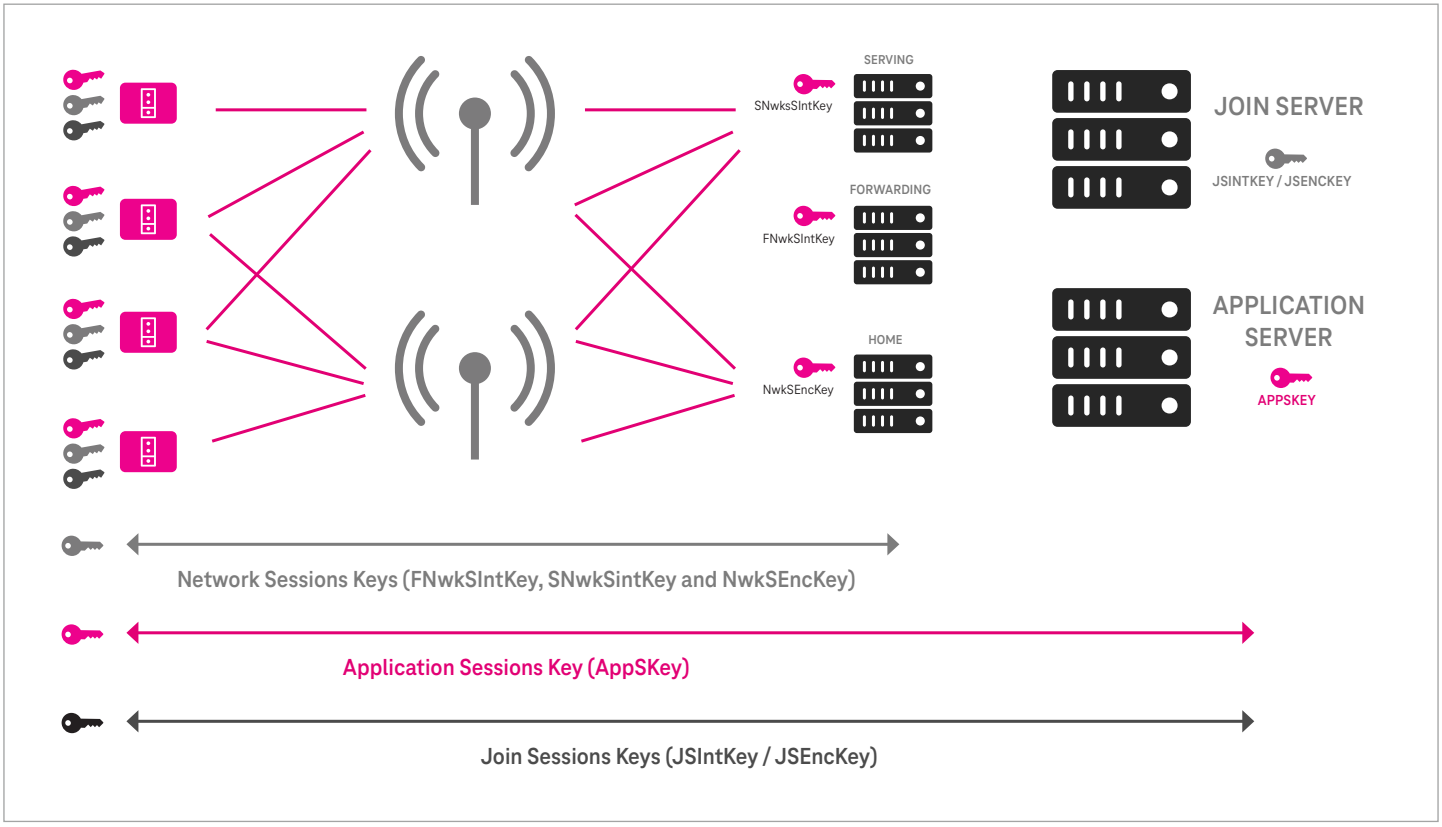


Figure 6: LoRaWAN architecture v1.1 (release 2017) [16]

LoRaWAN v1.1				
Key	Description	Required in Joining Type		Generation
		OTAA	ABP	
Keys needed before activation				
NwkKey	Is used for MIC for join-request packets, to encrypt join-accept packets, and derive all network session keys.	Yes	No	Stored beforehand
AppKey	Is used to derive AppSKey	Yes	No	Stored beforehand
JSIntKey	Is used for MIC of rejoin-request and join-accept packets	Yes	No	OTAA: generated from NwkKey and DevEUI
JSEncKey	Is used to encrypt join-accept triggered by rejoin-request	Yes	No	OTAA: generated from NwkKey and DevEUI
Keys needed after activation				
FNwkSIntKey	Is used for a part of the MIC for uplink data packets	Yes	Yes	ABP: manually generated OTAA: Generated from NwkKey and join-accept message
SNwkSIntKey	Is used for the MIC of all downlink data packets and for a part of the MIC for uplink packets	Yes	Yes	ABP: manually generated OTAA: generated from NwkKey and join-accept message
NwkSEncKey	Is used to encrypt all downlink and uplink MAC packets	Yes	Yes	ABP: manually generated OTAA: generated from NwkKey and join-accept message
AppSKey	Is used to encrypt/decrypt payload of data packets	Yes	Yes	ABP: manually generated OTAA: generated from AppKey and join-accept message
Identifiers				
JoinEUI	64-bit globally unique application ID that identifies the join server	Yes	No	Stored beforehand
DevEUI	64-bit globally unique device ID assigned by the network server	Yes	No	Stored beforehand
DevAddr	32-bit unique device address in the current network	Yes	Yes	ABP: manually generated OTAA: received by join-accept message

Table 7: Security keys and identifiers in a LoRaWAN architecture v1.1 [20]

3.3.1 Vulnerabilities of LoRaWAN v1.1

Many critical vulnerabilities from LoRaWAN architecture v1.0 have been fixed in v1.1. But the new architecture is not without vulnerabilities or security risks. One of the main weaknesses is still the endpoints: their firmware can be changed, and the devices thus be manipulated. Furthermore, an adversary could succeed in extracting secret keys from a device since many device manufacturers still do not implement secure elements due to their high prices. However, scientific research on architecture v1.1 has disclosed further security risks. For instance, the join-accept message is still encrypted through AES-128 in the unrecommended ECB mode. Even worse, in contrast to v1.0, key generation now requires the use of an operation mode too and relies on ECB mode [19]. Butun et al. [16] highlighted that re-keying of the master keys is still not possible. They also evaluated several possible attacks[2] and identified the following ones to have the highest risk in one of the four categories confidentiality, integrity, availability, and authentication and access control:

- **Device cloning or firmware replacement:** An adversary with physical access to a LoRaWAN device could flash the firmware or extract keys. Since such an attack is easy to perform, hard to detect and probably highly attractive to cyber criminals, the risk at authentication and access control is considered critically high.
- **Self-Replay Attack:** An attacker observes a join-request message and interrupts the transmission of the corresponding join-accept message through RF jamming. After a timeout, the end device will resend the join-request and the response is again prevented. This attack will thus diminish the availability of the network.
- **Rogue endpoint attack:** An adversary introduces an authentic-looking but rogue end device into a LoRaWAN network, for instance by reusing key material extracted from a valid device. The rogue device could be used to jam the network, to inject false data in the application server, or to replay packets and thus decrease a gateway's availability. Especially, the risk for authentication and access control is considered critically high.

[2] For the detailed risk analysis on possible LoRaWAN v1.1 attacks see [16].

4. Security of NB-IoT

Narrowband-IoT (NB-IoT) is a cellular IoT technology that is operated in licensed spectrum. As the name suggests, NB-IoT uses narrowband frequencies. These can be used because all functions that are not needed (e.g. voice transmission) have been removed. Hence, data packets are as small as possible, and low power consumption is possible. NB-IoT is based on the LTE standard and thus benefits from the tested and approved security mechanisms of LTE. These are ensured through standardization by 3GPP.

4.1. Modulation: OFDMA/ SC-FDMA

NB-IoT uses either GSM or LTE frequency spectrum [1]. The modulation technology is different for uplink and downlink. Downlink transmissions rely on Orthogonal Frequency Division Multiplex Access (OFDMA) based on Quadrature Amplitude Modulation with 64 different symbols (64QAM). OFDMA divides the available frequency band into a multitude of small subchannels. The data to be transmitted is then split into several data streams that are submitted via the subchannels in parallel. The use of many subcarriers makes the OFDM method very robust since disturbances on specific frequencies do not affect the complete data stream [21]. The 64QAM modulation provides 64 signal states consisting of different combinations of amplitude and phase. This allows the transmission of 6 bits per symbol, and thus supports higher data rates as lower order modulation schemes such as 16QAM. For uplink transmissions, NB-IoT uses Single-Carrier Frequency Division Multiple Access (SC-FDMA) with 64QAM since this method is more energy-efficient and thus increases the battery lifetime within the end devices. While SC-FDMA is derived from ODFMA, it only uses one carrier: instead of transmitting data symbols in parallel, each data symbol is spread over the available spectrum [22].

The physical layer of LTE and thus NB-IoT is well-described by the 3GPP standards. This, for instance, facilitates attacks such as RF jamming for possible attackers (see also [23]). Furthermore, it is quite easy and cost-efficient to set-up a rogue base station for LTE today and receive LTE signals due to the availability of software-defined radios, appropriate open-source software, and cheap antennas. However, LTE networks apply mutual authentication between end devices and base stations (as described in Chapter 4.2.1 below), and are thus not as prone to fake-base-station attacks as GSM.

Advantages:

- ⊕ **Robustness** against disturbances
- ⊕ Ideal for low bandwidth applications and results in reduced latency and increased efficiency
- ⊕ Due to mutual authentication, hard to integrate false base stations in the network

Disadvantages:

- ⊖ **RF jamming** is possible
- ⊖ **Fake base stations** are easy to create but hard to integrate in a network due to mutual authentication

Table 8: Advantages and disadvantages of OFDMA/SC-FDMA

4.2. NB-IoT architecture

The architecture of NB-IoT is based on the LTE architecture. The overall architecture of the underlying LTE system is called an Evolved Packet System (EPS). The EPS is an IP-based network with clearly defined interfaces. It was introduced with the first LTE standard (3GPP Release 8) in December 2008 and has since been continuously expanded. Figure 12 shows the EPS components relevant for NB-IoT. This architecture is also known as the 3GPP Cellular IoT (CIoT) network.

The user equipment (UE) consists of a terminal device – in this case a NB-IoT device – and a SIM card (including the UICC hardware and the USIM application). The UE connects to the base station (eNodeB) via the LTE-Uu radio interface. The user plane data is then transmitted via the S1-U interface to the Serving Gateway (SGW) of the EPC. User data transmitted via the user plane is routed from the Packet Data Network Gateway (PGW) to the CIoT Application Server. The control plane data is transferred to the Mobility Management Entity (MME) via the S1-MME Interface. Depending on the vendor, the functions from control plane nodes (MME) and user plane nodes (SGW, PGW) can be consolidated into a component called C-SGN (CIoT Serving Gateway Node). If user data is transferred via the control plane, the Service Capability Exposure Function (SCEF) (if implemented in the core network) provides a RESTful API for transferring the payload. The data transfer for the downlink is performed vice versa.

One distinction included in the 3GPP specifications is especially important to understand NB-IoT security. The cellular protocols are divided into the Access Stratum (AS) and the Non-Access Stratum (NAS):

- The AS includes all protocols for communication between UE and eNodeB via the radio interface. It therefore includes protocols for user and control plane.
- The NAS is all non-radio signaling traffic between UE and MME, and merely corresponds to control plane protocols [24].

Control plane protocols are usually used for signaling and control tasks only. However, the transmission of small data amounts via the user plane can be inefficient. Therefore NB-IoT allows transmission of small user data via the control plane too – with or without TCP/IP header. This technology is called Data over NAS [25].

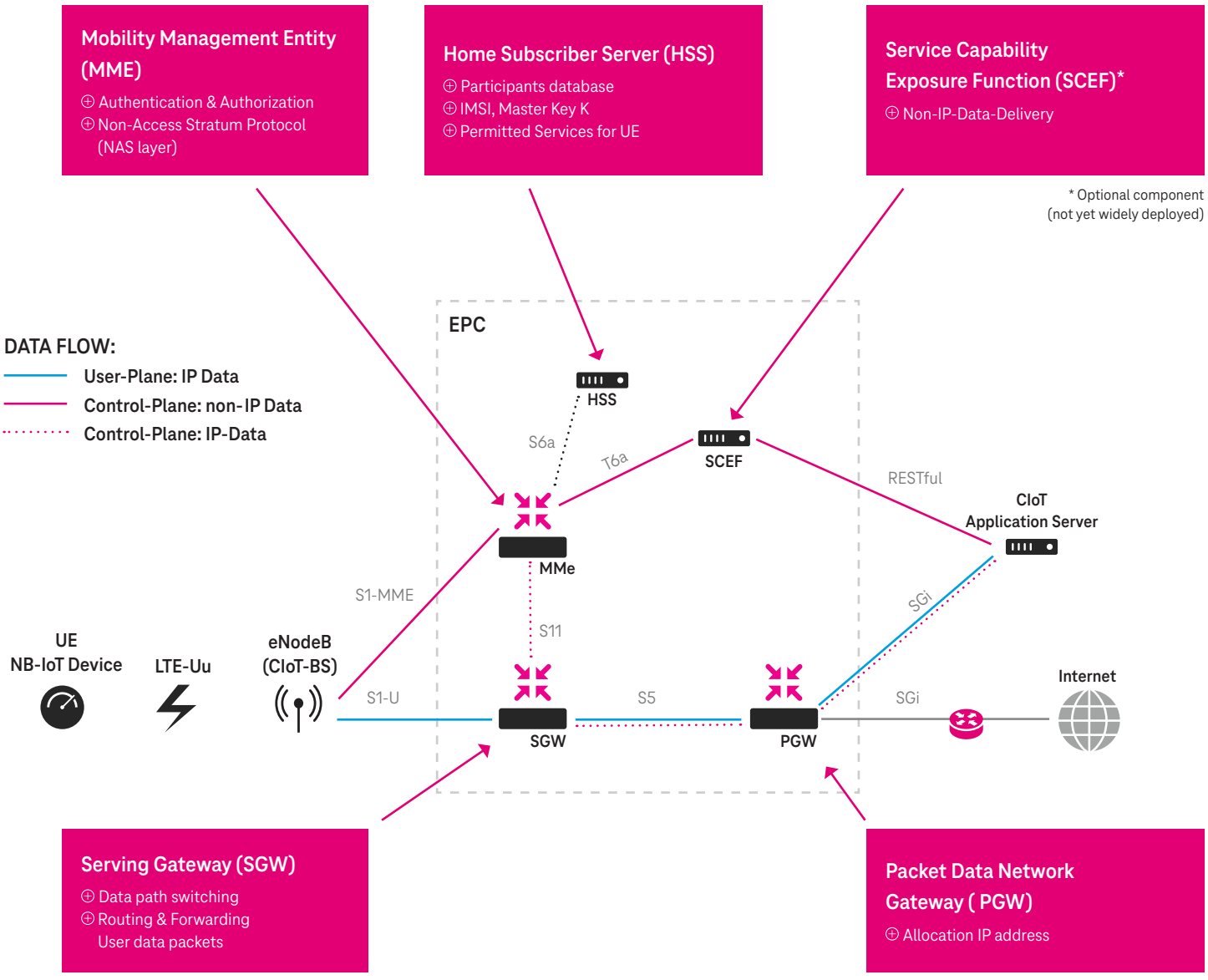


Figure 8: Evolved Packet System (EPS) for LTE/NB-IoT [26]

4.2.1. Initial attach procedure for NB-IoT devices

The process of connecting a device to a NB-IoT network for the first time is called initial attach procedure. It includes two steps essential for NB-IoT security: mutual authentication and key agreement (see Figure 9).

Mutual authentication

To establish a secure connection between an end device and the NB-IoT network, both parties must authenticate to each other. For this purpose, the USIM contains a unique identification number that includes the IMSI as well as a 128-bit long master key K. The HSS stores every valid SIM, its master key K and its authorizations. For mutual authentication, the end device and HSS prove that they possess the master key. However, to be precise, it is the USIM – not the device or the user – that authenticates itself towards the network.

The end device first sends an Attach Request command with its IMSI to the MME. The MME thereupon requests an authentication vector (AV) from the HSS. The HSS generates the authentication vector from the master key K, a counter (SQN) and a random nonce (RAND). The final vector includes RAND, a token for network authentication (AUTN), an expected response during user authentication (XRES) and a key (KASME). After receiving the authentication vector from the HSS, the MME forwards RAND and AUTN to the user's USIM. The USIM checks MAC and freshness of the received AUTN (by checking that SQN is higher than last one used and calculates CK, IK). Then USIM calculates RES and sends RES back to MME. CK, IK are used to calculate KASME by the UE. The MME compares RES with XRES. If both values are equal, the network and USIM have proven to be in possession of the secret key K. If the user authentication fails, the connection to the user equipment is terminated.

Key generation

If the mutual authentication succeeds, a secure data communication can be established. Depending on the Home PLMN operators policy, the integrity and encryption algorithms to be used are agreed upon during the Initial Attach and are based on the device's and network's capabilities. During key agreement, unnecessary transfers of keys are avoided. Instead, the keys are generated separately by the affected parties, and only after a successful authentication procedure.

From the key KASME, two keys are derived for integrity and confidentiality protection: KNASenc and KNASint. These keys are used to securely set up the NAS layer of the control plane. Furthermore, the MME generates the key KeNB from KASME, and sends it to the eNodeB. The UE derives the same key independently. UE and eNode B now generate the integrity key KRRCint and the encryption key KRRCenc, which are used to secure the AS layer of the control plane. The control plane can thus be completely secured between the mobile device and MME. To protect the user plane, UE and eNodeB calculate the encryption key KUPenc. This ensures the confidentiality of the user plane between these two components. In addition, MNOs can decide to implement an IPsec tunnel from the base station to the core network. This is the case for the German Deutsche Telekom network, for instance. An IPsec tunnel is very secure due to confidentiality and integrity protection as well as authentication of communication endpoints. [9]

Secure SIM card protects key material

In contrast to many LoRaWAN end devices, NB-IoT devices are equipped with a SIM card that is a secure element and thus tamper-resistant. Hence, cryptographic data such as the master key K can not be extracted from a Deutsche Telekom SIM. [24] Furthermore, Deutsche Telekom has developed a secure SIM designed for low-cost IoT devices together with leading industry partners: the nuSIM is an integrated SIM that ensures low cost and power consumption while maintaining LTE-grade security [1]. SIM manufacturers are regularly certified by the GSMA and work with high-security data centers.

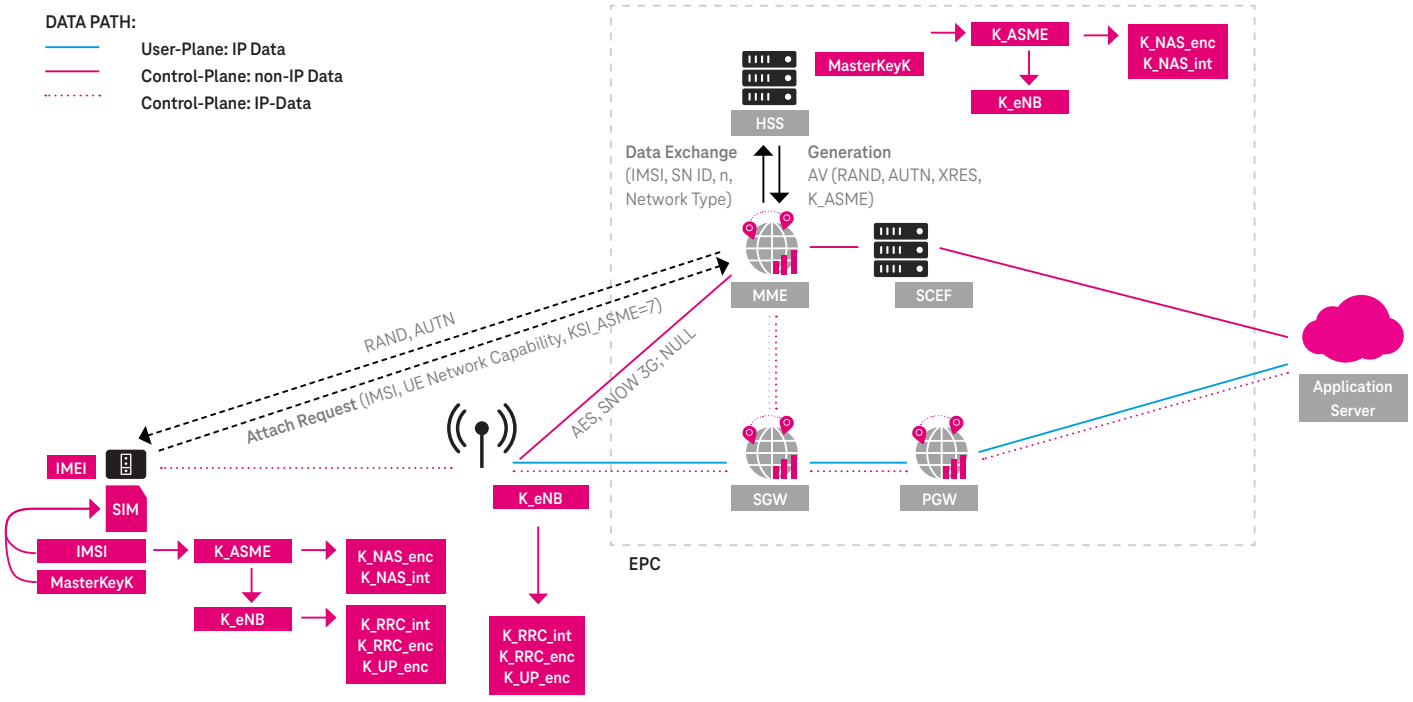


Figure 9: Attach request and key agreement/exchange

Advantages of the NB-IoT Initial Attach procedure

Advantages:

- **Explicit mutual authentication** based on pre-shared key in SIM and HSS
- **Secure key generation**
- **SIM is a secure element**

4.2.2. Data transmission

The protocol stack of NB-IoT categorized by control and user plane can be seen in Figure 11. The layer 1 and 2 protocols PHY, MAC and PLC of the air interface are not protected. However, in NB-IoT networks, the connection between UE and eNodeB is secured at PDCP layer (part of layer 2) by the Access Stratum (AS) security setup. On the user plane, IP packets are protected through encryption. However, the 3GPP specification defines that user plane packets shall not be integrity-protected on the air interface. In contrast, on the control place the AS secures the transmission of RRC packets by both an integrity and encryption algorithm.

Thanks to the Non-Access Stratum (NAS) Security Setup, the control plane has an additional upper-layer security level. While the Access Stratum terminates at the eNode B, the NAS protocol protects the integrity and confidentiality of the connection between UE and MME. Although both NAS and AS support encryption, 3GPP does not prescribe confidentiality protection. Instead, this is depending on regulatory restrictions and left as an option for the network operator. [9] [24] Since the control plane of LTE networks is better protected than the user plane, Deutsche Telekom customers always use the control plane for NB-IoT pay-load data. This is also common for other operators. Hence, it is not only encrypted but also protected against manipulation – on two layers instead of one.

For securing communication between base station and core network, Deutsche Telekom additionally uses security tunnels. Additional network and secure transport protocols (e.g. IPSec tunnels) are used to connect customers' premises infrastructure to the core network.

Thanks to the Non-Access Stratum (NAS) Security Setup, the control plane has an additional upper-layer security level. While the Access Stratum terminates at the eNode B, the NAS protocol protects the integrity and confidentiality of the connection between UE and MME. Although both NAS and AS support encryption, 3GPP does not prescribe confidentiality protection. Instead, this is depending on the network operators policy and shall also follow regulatory compliance. [9] [24] Since the control plane of LTE networks is better protected than the user plane, Deutsche Telekom customers always use the control plane for NB-IoT pay-load data. This is also common for other operators. Hence, it is not only encrypted but also protected against manipulation – on two layers instead of one

Although the specification does not define end-to-end encryption, it is possible to implement it using the Datagram Transport Layer Security (DTLS) protocol or the more power-efficient BEST protocol (see also Chapter 2). BEST, however, is not yet offered. Apart from the 3GPP feature for end-to-end encryption, other solutions are introduced by open standrad organizations as well as hardware and cloud vendors.

Cipher ID	Method	Integrity ID	Method
EEA0	NULL (no encryption)	EIA0	NULL (no integrity)
EEA1	SNOW 3G	EIA1	SNOW 3G
EEA2	AES-CTR	EIA2	AES CMAC

Table 9: Encryption and integrity schemes in NB-IoT networks [9]

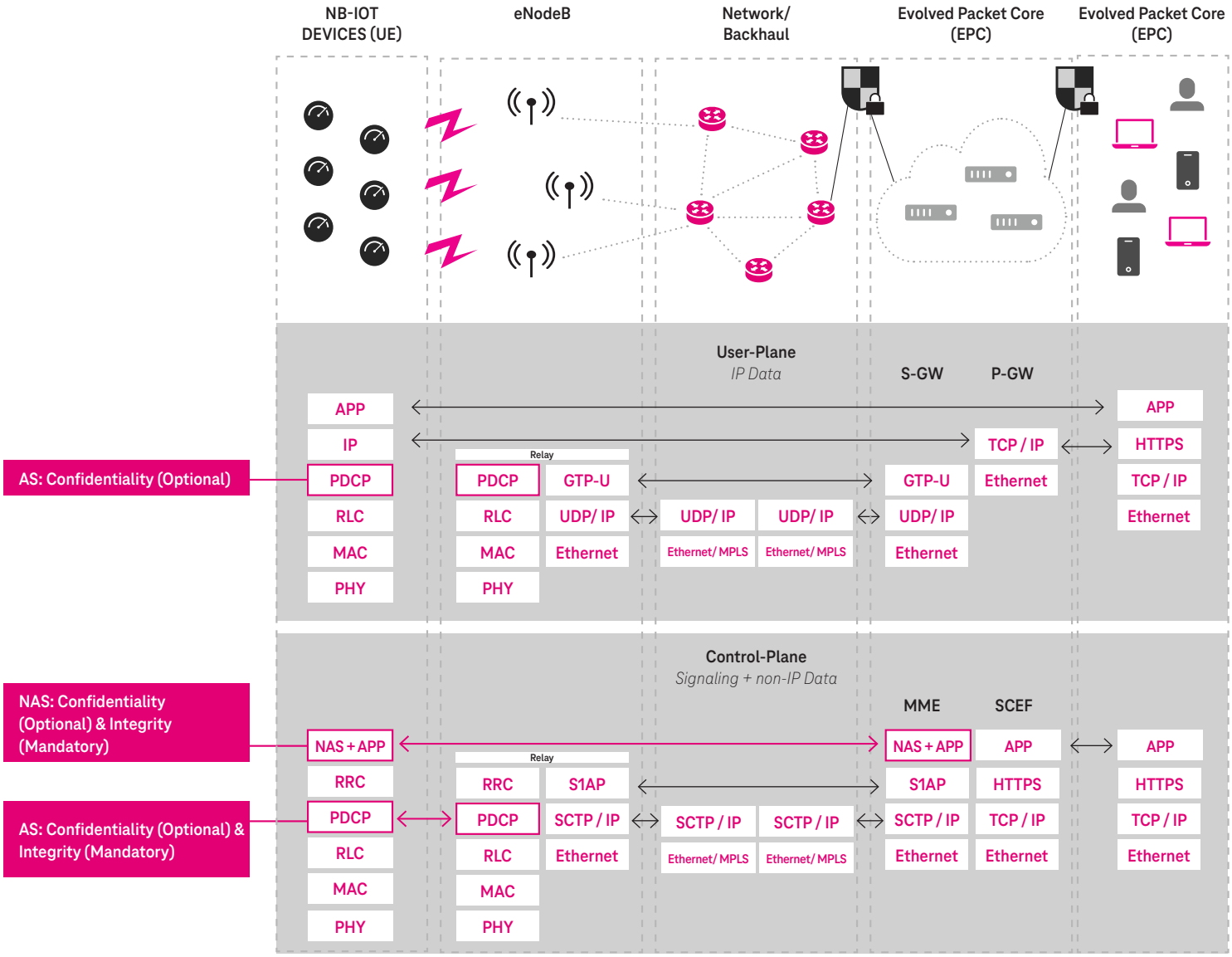


Figure 10: Protocol stack and security mechanism LTE/NB-IoT [26]

Advantages:

- ⊕ **Encryption** available for user and control plane on the air interface, and for the control plane between UE and MME
- ⊕ **Data over NAS** allows user data to be sent more securely via the control plane

Disadvantages:

- ⊖ **The choice of one of four encryption algorithms** is left to the network operator
- ⊖ **No integrity protection** for the user plane
- ⊖ **No end-to-end encryption**

Table 10: Advantages and disadvantages of NB-IoT data transmission

4.2.3 Vulnerabilities of NB-IoT

LTE networks and thus NB-IoT are designed to have a high level of security. Especially in contrast to GSM, they benefit from the mutual authentication between end device and network, the use of public, extensively tested cryptographic algorithms and a secure key generation and distribution. Another advantage is the secure storage of keys in the SIM card.

However, the risk of successful cyber attacks on LTE can only be mitigated. As already mentioned above, 3GPP leaves encryption as an option to MNOs and even prohibits integrity protection of user plane traffic. According to the US-American NIST institute, RF jamming attacks against LTE networks are feasible. Furthermore, NB-IoT and LTE LTE often coexist with less secure UMTS (3G) or GSM (2G) networks. Hence, an end device should be able to connect to a 3G or 2G network if no LTE access is available. This, however, increases the attack surface. For call signaling in GSM and UMTS, a separate network is used that also enables roaming: the SS7 network. SS7 had several security issues in the past. Some of them are overcome in LTE roaming but still some issues remain open.

NB-IoT networks heavily rely on IP technology. IP is widely known among both security experts and cyber criminals. This can be an advantage and a disadvantage. On the one hand, well approved IP security technologies exist and can be implemented to secure NB-IoT. On the other hand, attackers know the weaknesses of IP networks and have appropriate tools ready. [24]

5. Conclusion

In summary, both NB-IoT and LoRaWAN have strong security mechanisms (see also Table 11). NB-IoT is an open standard by the 3GPP and based on LTE. Thus, it heavily benefits from its security mechanisms being based on the LTE radio standard: the security concept has been developed and tested in much greater depth. LoRaWAN is a protocol defined by the LoRa Alliance based on a proprietary modulation. Yet, it has essential security features. While NB-IoT uses licensed spectrum, LoRaWAN relies on unlicensed spectrum. LoRaWAN is thus more prone to RF jamming, although it has a very robust modulation.

The process of integrating an end device into an NB-IoT network is well secured by the LTE Initial Attach procedure including mutual authentication and secure key generation. Furthermore, the keys are distributed in a highly secure way thanks to tamper-proof USIMs and SIM vendors that are regularly certified by the GSMA and use high-security data centers. LoRaWAN has two options for this join process. One of these, ABP, is insecure and not recommended. OTAA, on the other hand, has important security features but flaws in the most widely used version v1.0. In particular, this includes the key generation process.

As regards encryption, LoRaWAN provides end-to-end encryption. The only drawback is that the intermediate network server generates the encryption key for application data in v1.0. The NB-IoT standard includes only optional encryption for user plane and control plane on the air interface, and for the control plane between end device and MME too. However, these encryption options are mandatory in Deutsche Telekom NB-IoT networks. End-to-end encryption can be implemented using DTLS or the upcoming and power-efficient BEST standard. In addition, the end-to-end encryption on the application layer is possible using OSCORE protocol, which is especially well suited for IoT frameworks using CoAP, such as OMA Specworks Lightweight M2M (LwM2M) and Open Connectivity Foundation/IoTivity (OCF) [27]. This is recommended mainly for roaming and security-sensitive applications, since providers such as Deutsche Telekom already use additional security mechanisms (e.g. IPsec tunnels) between the core network and application servers. LoRaWAN uses the secure encryption scheme AES-128. For NB-IoT, providers can choose between different algorithms. Deutsche Telekom, for instance, uses AES too.

Integrity is ensured for complete LoRaWAN frames between end device and network server, and thus not end-to-end. In NB-IoT networks, integrity protection is limited to the control plane, and applied between end device and base station as well as between end device and MME. However, Deutsche Telekom transmits NB-IoT data via the control plane – thanks to the Data over NAS technology – hence applying integrity also for user data.

For NB-IoT use cases, it can be assumed that the MNO has a well-rounded security concept in their home network. The constant work of 3GPP as well as security researchers all over the world means that LTE security – and thus NB-IoT security – is constantly improved. The security of LoRaWAN networks, on the other hand, heavily depends on the comprehensive use of LoRaWAN architecture v1.1. , which is still not commonly deployed as of today.

Independently from the technology, the secure implementation of features and the correct and secure construction of systems become more and more relevant. Hence, organizations should always question the security concept and conduct individual risk assessments and mitigations.

In sum, the crucial advantage of NB-IoT over LoRaWAN is the secure storage of the cryptographic keys as a standard. This means: while NB-IoT keys are unlikely to be extracted from the SIM or the manufacturers' data centers, many LoRaWAN devices are not tamper-proof, thus possibly disclosing secret keys to black-hat hackers.

	LoRaWAN	NB-IoT
Standardization	• LoRaWAN (MAC layer): specification developed and maintained by LoRa Alliance • LoRa (physical layer): proprietary patented by Semtech	• Open standard by 3GPP • Based on LTE
Spectrum	• Non-licensed spectrum • Modulation based on the very robust and hard to receive Chirp Spread Spectrum (CSS)	• Licensed spectrum • Modulation based on the robust OFDMA/SC-FDMA schemes
Join methods	• ABP: fast but insecure due to persistent keys • OTAA: secure method besides small limitations, improved with LoRaWAN v1.1	• Initial Attack: secure attachment due to mutual authentication, and secure key generation and exchange
Encryption	• End-to-End encryption for frame payloads by default	• Encryption between end device and eNodeB at layer 2 of user and control plane • Encryption between end device and MME at NAS layer of the control plane • No end-to-end encryption by default but can be realized through DTLS, BEST or OSCORE, for instance
Encryption Algorithm	• AES-128 in CCM mode	• The MNO can select a stream cipher encryption algorithm, based on e.g. SNOW 3G, AES-128-CTR • AES-CTR is standard in Deutsche Telekom networks
Integrity	• Integrity protection of header and payload of MAC frames between end device and network server • No integrity between network and application server	• Integrity protection between end device and eNodeB at layer 2 and between end device and MME at NAS layer of the control plane • No integrity protection of the user plane but feature that allows the transport of user data via the more secure control plane
Integrity Algorithm	• AES-128-CMAC	• The MNO can select an encryption algorithm, e.g. SNOW 3G, AES-128-CMAC (used by Deutsche Telekom)
End device security	• **Mostly no secure key storage** due to the lack of a secure element in the LoRaWAN end device	• **Secure element** in the SIM card protects keys from extraction • **Certified high-security data centers** used by SIM manufacturers
Vulnerabilities	• **RF jamming attacks** are easier than in licensed spectrum • **Physical attacks** are critical but easily detectable • **Architecture v.1.0** has several known security flaws (e.g. limited end-to-end encryption through temporary possession of key by intermediate network server) but is still the most widespread architecture. • **Architecture v.1.1** has improved but firmware replacement is still possible as well as self-replay attacks and rogue endpoint attacks	• **In roaming protocols** security flaws have been detected in the past • **Forcing devices to use GSM** is a risk • **RF jamming attacks** are feasible • **Rogue base stations** are easy to build but hard to integrate into a valid network

Table 11: Summary of security features in NB-IoT and LoRaWAN

III. Sources

[1] ..... Deutsche Telekom, Mobile IoT guide – how NB-IoT and LTE-M are helping the IoT take off. Bonn, 2019. [Online] Available: https://iot.telekom.com/resource/blob/data/177214/02ccc79436c73ed5a6632ff-c04a438d6/mobile-iot-guide-2019.pdf

[2] ..... Statista, Number of LPWAN connections by technology worldwide from 2017 to 2023 . [Online] Available: https://www.statista.com/statistics/880822/lpwan-ic-market-share-by-technology/

[3] ..... LoRa Alliance. (2015). LoRaWAN – What Is It?: A Technical Overview of LoRa and LoRaWAN. Retrieved from https://lora-alliance.org/sites/default/files/2018–04/what-is-lorawan.pdf

[4] ..... Daemen, J., Rijmen, V. (2003). AES Proposal: Rijndael. National Institute of Standards and Technology. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf#page=1

[5] ..... United States National Institute of Standards and Technology. (2001). Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[6] ..... Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, D., Ferguson, N., Kohno, T., Stay, M. (2000). The Twofish Team's Final Comments on AES Selection. https://www.schneier.com/academic/paperfiles/paper-twofish-final.pdf

[7] ..... H. Knospe, A Course in Cryptography in Pure and Applied Undergraduate Texts, vol. 40., Providence, Rhode Island: American Mathematical Society, 2019.

[8] ..... Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs), IEEE 802.15.4–2006, IEEE, 2006, New York.

[9] ..... 3GPP System Architecture Evolution (SAE); Security architecture (Release 16), TS 33.401 V16.3.0, 3GPP, 2020, Valbonne.

[10] ..... G. Orhanou et al., "EPS confidentiality and integrity mechanisms algorithmic approach" in IJCSI International Journal of Computer Science Issues, vol. 7, issue 4, no 4, Jul. 2010, pp. 15–23

[11] ..... Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification, ETSI/SAGE Specification, Version 1.1, 2006. https://www.gsma.com/aboutus/wp-content/uploads/2014/12/snow3gspec.pdf

[12] ..... Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST) (Release 15), TS 33.163 V16.2.0, 3GPP, 2019, Valbonne.

[13] ..... Semtech Acquires Wireless Long Range IP Provider Cycleo. (2012). Retrieved from https://www.design-reuse.com/news/28706/semtech-cycleo-acquisition.html

[14] ..... Schmidiger GmbH. (n.d.). Wie gut ist die Funktechnologie LoRa wirklich?. Retrieved from https://www.schmidiger.ch/blog/lora-funktechnologie-wie-gut-ist-sie-wirklich

[15] ..... LoRaWAN™ 1.0.3 Specification, LoRa Alliance, 2018, Beaverton.

[16] ..... Butun, I.; Pereira, N.; Gidlund, M. (2018). Security Risk Analysis of LoRaWAN and Future Directions. Future Internet. 11(1), 3. https://doi.org/10.3390/fi11010003

[17] ..... You, I., Kwon, S., Choudhary, G., Sharma, V., Seo, J. (2018). An Enhanced LoRaWAN Security Protocol for Privacy Preservation in IoT with a Case Study on a Smart Factory-Enabled Parking System

[18] ..... Schloten, E. (2019). Sicherheit in LoRaWAN Netzen – ein Überblick.

[19] ..... LoRaWAN™ 1.1 Specification, LoRa Alliance, 2017, Beaverton.

[20] ..... Haxhibeqiri, J., De Poorter, E., Moerman, I., Hoebeke, Jn. (2018). A Survey of LoRaWAN for IoT: From Technology to Application.

[21] ..... Elektronikkompendium, OFDM - orthogonal frequency division multiplex. [Online] Available: https://www.elektronik-kompendium.de/sites/kom/1509011.htm

[22] ..... 3GPP, LTE. [Online] Available: https://www.3gpp.org/technologies/keywords-acronyms/98-lte

[23] ..... T. Pushpalata et al., "Need of physical layer security in lte: analysis of vulnerabilities in LTE physical layer" in 2015 IEEE Bombay Section Symposium (IBSS), Mumbai, 2015, pp. 1–5.

[24] ..... J. Cichonski et al., Guide to LTE security. NIST special publication 800–187, 2017. [Online] Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800–187.pdf

[25] ..... GSMA, Security features of LTE-M and NB-IoT networks. United Kingdom, 2019. [Online] Available: https://www.gsma.com/iot/resources/security-features-of-ltem-nbiot/

[26] ..... Markus Schober. (2020). Masterarbeit FH Salzburg: Evaluierung von LPWAN Technologien für den Einsatz in einem Multi-Utility Unternehmen.

[27] ..... Ericsson. OSCORE: A look at the new IoT security protocol. [Online] Available: https://www.ericsson.com/en/blog/2019/11/oscore-iot-security-protocol

Note: All the above web resources have been accessed between August and September 2020.

Contact
iot@telekom.de
iot.telekom.com

Publisher
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn, Germany

Version 1.0, January 2021