Vergleich und Analyse der Sicherheitsaspekte von LoRaWAN und NB-IoT

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

LIFE IS FOR SHARING.

Deutsche Telekom IoT
connect. digitize. get ahead.

Inhalt

I. Abkürzungen

3GPP ..... 3rd Generation Partnership Project
64QAM ..... Quadrature Amplitude Modulation 64 Symbole
AES ..... Advanced Encryption Standard
AKA ..... Authentication and Key Agreement
App ..... Anwendung
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 ..... Netzwerk
NwkSEncKey ..... Network Session Encryption Key
NwkSKey ..... Network Session Key
OFDM ..... Orthogonales Frequenzmultiplexverfahren
OSCORE ..... Object Security for Constrained RESTful Environments
PDCP ..... Packet Data Convergence Protocol
RF-Störung ..... Funkfrequenzstörung
RRC ..... Radio Resource Control
SNwkSIntKey ..... Serving Network Session Integrity Key
UE ..... Nutzerendgerät
UICC ..... Universal Integrated Circuit Card
UMTS ..... Universal Mobile Telecommunications System
UP ..... User plane
USIM ..... Universal Subscriber Identity Module
XOR ..... exklusiv-ODER-Operation

II. Management Summary

NB-IoT und LoRaWAN sind die beiden gängigsten Low-Power-Wide-Area-Technologien (LPWA) und bieten energieeffiziente Mobilkonnektivität mit großer Reichweite für intelligente Geräte, wie etwa Smart Meters, einfache Tracker und Sensoren für Maschinen und Container. Da Black-Hat-Hacker zunehmend Interesse am Internet der Dinge zeigen, vergleicht dieses Dokument die Sicherheit von NB-IoT und LoRaWAN.

LoRaWANs, mit der am häufigsten verwendeten Architektur v1.0, bestehen aus den Endgeräten, den Gateways, mit denen sie drahtlos verbunden sind, einem Netzwerkserver und einem Anwendungsserver. Der Prozess der Integration neuer Geräte in ein Netzwerk ist gut gesichert, wenn die sogenannte Over-the-Air-Activation-Methode verwendet wird. Es gibt nur geringfügige Nachteile, beispielsweise die Verwendung einer überholten Verschlüsselungsbetriebsart.

Im Hinblick auf die Datenübertragung gewährleistet LoRaWAN 1.0 Integrität für komplette Nachrichten, aber nicht zwischen Netzwerkserver und Anwendungsserver. Ende-zu-Ende-Verschlüsselung der Frame-Payloads wird standardmäßig bereitgestellt. Dabei gibt es jedoch eine Schwachstelle: Der Netzwerkserver – nur ein Zwischenpunkt in der Anwendungskommunikation – gelangt während des Verbindungsprozesses der Endgeräte in den Besitz des Verschlüsselungsschlüssels der Anwendung. Diese Schwachstelle wurde durch die neue, im Jahr 2017 eingeführte Architektur v1.1 korrigi-ert. Viele weitere Sicherheitslücken wurden durch dieses Update geschlossen. Leider wird v1.1 nach wie vor kaum genutzt.

Auf der physischen Schicht verwendet LoRaWAN unlizenzierte Frequenzbänder. Dadurch wird die Durchführung einer Funkfrequenzstörung (RF-Störung) einfach. LoRaWAN verwendet jedoch die sehr robuste LoRa-Modulation. LoRa greift auf eine konstant wechselnde Frequenz zurück. Damit wird es für einen Angreifer bereits äußerst schwierig, Daten von Interesse zu empfangen.

Die kritischste Schwäche von LoRaWAN sind die Endgeräte: Aus Kostengründen weisen sie normalerweise kein sicheres Element auf – einen Chip, der kryptografische Informationen wie geheime Schlüssel sicher speichert. Somit kann ein Angreifer bei der Extraktion von geheimen Schlüsseln oder beim Flashen des Geräts mit kompromittierter Firmware Erfolg haben.

NB-IoT basiert auf LTE, wie durch das 3GPP der internationalen Standardisierungsgremien spezifiziert. Somit profitiert NB-IoT von den sorgfältig entwickelten und getesteten LTE-Sicherheitsfunktionen. Dazu gehören gegenseitige Authentifizierung von Endgerät und Netzwerk, bekannte kryptografische Algorithmen wie AES sowie eine sichere Schlüsselgenerierung und ein sicherer Schlüsselaustausch. Die Luftschnittstelle von NB-IoT ist auf Benutzer- und/oder Kontrollebene verschlüsselt. Es gibt jedoch standardmäßig keine Ende-zu-Ende-Verschlüsselung. Netzbetreiber können aber ein höheres Sicherheitsniveau einführen, indem sie beispielsweise Sicherheitstunnel (IP-VPNs) vom Kernnetzwerk zum Anwendungsserver einsetzen. Zudem kann man eine Ende-zu-Ende-Verschlüsselung einrichten über das DTLS-Protokoll oder künftig über die energieeffizienten Protokolle wie BEST (3GPP-Standard), OSCORE (LWM2M) oder proprietäre Lösungen.

Die 3GPP-Spezifikation begrenzt den Integritätsschutz auf die Kontrollebene. Glücklicherweise ermöglicht NB-IoT die Übertragung kleiner Benutzerdaten über die Kontrollebene und macht sie dennoch resistent gegen Manipulation. Ein großer Vorteil liegt darin, dass NB-IoT-SIM-Karten manipulationssicher sind: Sie enthalten ein sicheres Element. Die Extraktion von Schlüsselmaterial ist damit sehr schwierig und in den meisten Fällen unwahrscheinlich.

Ein Risiko in Mobilfunknetzen besteht darin, dass ein Angreifer ein Endgerät zwingen kann, den weniger sicheren 2G-Mobilfunkstandard zu nutzen, indem er vorgibt, dass kein LTE zur Verfügung steht. Zusätzliche Sicherheitsmaßnahmen, wie etwa Ende-zu-Ende-Verschlüsselung, sollten für das Roaming in NB-IoT-Netzwerken implementiert werden, da verschiedene Schwachstellen beim Roaming in der Vergangenheit angesprochen wurden. Wenn ein NB-IoT-Anwendungsfall jedoch ausschließlich im Heimnetzwerk des Mobilfunknetzbetreibers stattfindet, sind keine zusätzlichen Sicherheitsmechanismen für die Übertragung erforderlich, da standardmäßig bereits ein hohes Sicherheitsniveau bereitgestellt wird.

Schlussfolgernd lässt sich sagen, dass beide LPWA-Technologien starke Sicherheit bieten, NB-IoT jedoch in einem äußerst wichtigen Aspekt LoRaWAN überlegen ist: der sicheren Speicherung der kryptografischen Schlüssel. Die Nutzung von Geräten ohne ein sicheres Element mindert die Effektivität der Ende-zu-Ende-Verschlüsselung. Unternehmen, die LoRaWAN verwenden, wird daher empfohlen, ein Sicherheitskonzept zu entwickeln. Dieses Konzept sollte Endgeräte mit einem sicheren Element, die sichere OTAA-Verbindungsmethode sowie die neueste LoRaWAN-Architektur v1.1 vorschreiben. Die Sicherheitsmechanismen von NB-IoT basieren auf dem LTE-Funk-standard. Dieser gewährleistet ein hohes Sicherheitsniveau. Denn-och sollte grundsätzlich Verschlüsselung zum Einsatz kommen, und kritische Benutzerdaten sollten über die sicherere Kontrollebene
(Daten über NAS) gesendet werden, wie es bei den meisten Betreibern bereits Standard ist. Zusätzliche Sicherheit ist für Roaming in Erwägung zu ziehen.

1. Einleitung

Das Internet der Dinge (Internet of Things, IoT) wächst kontinuierlich. Eine beträchtliche Anzahl an Anwendungsfällen greift auf preiswerte IoT-Geräte mit langen Akkulaufzeiten zurück. Dies gilt beispielsweise für Smart Cities, vorbeugende Wartung oder Smart Metering. Die zweite wichtige Komponente solcher Anwendungsfälle sind Mobilfunknetze, die Daten energieeffizient über weite Entfernungen zu akzeptablen Kosten übertragen: Low-Power-Wide-Area-Netzwerke (LPWA).

Die beiden am häufigsten verwendeten LPWA-Technologien sind NarrowBand IoT (NB-IoT) und Long Range Wide Area Network (Lo-RaWAN). NB-IoT basiert auf LTE und wurde 2016 durch die Standard-isierungsorganisation für Mobilfunktechniken 3rd Generation Part-nership Project (3GPP) standardisiert. Netzwerke dieser Art werden in einem lizenzierten Spektrum betrieben [1]. Die Menge der welt-weiten NB-IoT-Verbindungen wird auf 130 Millionen veranschlagt – und voraussichtlich 740 Millionen im Jahr 2023 erreichen. LoRaWAN hingegen wurde von der LoRa AllianceTM entwickelt, einem offenem Zusammenschluss von Unternehmen aus verschiedenen Sektoren, wie etwa Telekommunikation und Systemintegration. Der Standard wurde im Jahr 2015 eingeführt und definiert das Kommunikation-sprotokoll und die Systemarchitektur für ein LPWA-Netzwerk. Diese Technologie greift auf ein unlizenziertes Spektrum zurück. Die Anzahl der LoRaWAN-Verbindungen im Jahr 2020 liegt bei etwa 191 Millionen und man geht davon aus, dass sie im Jahr 2023 auf 731 Millionen steigt. [2] [3]

Während immer mehr IoT-Anwendungsfälle die NB-IoT- oder LoRaWAN-Technologie nutzen, beobachten Sicherheitsspezialisten seit Jahren einen starken Anstieg IoT-bezogener Angriffe. Beispielsweise sind das Mirai Botnet und seine Derivate nach wie vor für eine große Anzahl der IoT-Malware-Angriffe verantwortlich. Daher beleuchtet dieses White Paper die Sicherheit von NB-IoT und LoRaWAN. Die Sicherheit der Technologien wird zunächst separat betrachtet. Das Dokument endet mit einem direkten Vergleich der Sicherheitsfunktionen beider LPWA-Technologien.

2. Wichtige Verschlüsselungs-verfahren

Im folgenden Kapitel werden wichtige Verschlüsselungsverfahren beschrieben, die bei LoRaWAN und NB-IoT zum Einsatz kommen.

AES

LoRaWAN und NB-IoT verwenden beide den Advanced Encryption Standard (AES), um Vertraulichkeit zu gewährleisten. AES ist eine weit verbreitete Verschlüsselungsmethode. Das Verfahren wurde 1998 veröffentlicht und im Jahr 2000 zertifiziert. Es handelt sich um eine symmetrische Verschlüsselungsmethode, bei der beide Kommunikationsparteien einen gemeinsamen geheimen Schlüssel verwenden. Daher sollte grundsätzlich sichergestellt werden, dass beide Parteien den geheimen Schlüssel in einer sicheren Weise erhalten. Unter der Annahme geeigneter Schlüssellängen geht man davon aus, dass AES rechnerisch sicher ist. Das bedeutet, dass die Verschlüsselung innerhalb eines akzeptablen Zeitraums auch mit sehr hoher Rechnerleistung nicht geknackt werden kann.

Die zu verschlüsselnde Blockgröße beträgt bei AES grundsätzlich 128 Bits. Lediglich die Schlüssellänge ist variabel. Übliche Schlüssellängen sind 128, 192 oder 256 Bits. Je größer die Schlüssellänge ist, desto sicherer, aber komplexer und energieintensiver ist die Verschlüsselung. Auch AES-128 wird jedoch heute als rechnerisch sicher betrachtet. [4,5,6] Künftig könnte aber die hohe Rechenleistung von Quantencomputern dazu führen, dass längere AES-Schlüssel erforderlich werden.

Es ist wichtig zu verstehen, dass die Sicherheit von AES auch stark von seiner Betriebsart abhängt. Die Betriebsart definiert, wie Nachrichten von mehr als 128 Bits – die somit aus mehreren Blöcken bestehen – verschlüsselt werden. AES unterstützt zahlreiche verschiedene Betriebsarten, die alle Vorteile und Nachteile aufweisen. Die gängigsten Modi werden nachfolgend beschrieben [7]:

Electronic Code Book Mode (ECB):

Im ECB-Modus wird jeder Block separat und unabhängig von anderen Blöcken verschlüsselt. ECB ist ein deterministisches Chiffrierverfahren: Die Verschlüsselung derselben Nachricht führt immer zu demselben Chiffretext. Das Design von ECB hat jedoch einen großen Nachteil: Nachrichtenmuster bleiben erhalten. Daher wird die Verwendung von AES im ECB-Modus nicht empfohlen.

Cipher Block Chaining Mode (CBC)

Der CBC-Modus greift auf eine nach dem Zufallsprinzip ausgewählte Binärzeichenfolge zurück, den sogenannten Initialisierungsvektor. Die Zeichenfolge wird mit dem ersten Nachrichtenblock mithilfe einer exklusiv-ODER-Operation (XOR) kombiniert und erst danach verschlüsselt. Für jeden folgenden Block wird die Nachricht vor der Verschlüsselung per XOR-Operation mit dem vorausgehenden Chiffretext verknüpft. Dank des Zufallsfaktors und der Abhängigkeit zwischen verschiedenen Chiffreblöcken leidet CBC nicht unter denselben Schwächen wie ECB. Ein Nachteil liegt jedoch darin, dass Fehler durch die Nachricht verbreitet werden können. Zudem ist CBC formbar. Das bedeutet, dass ein Angreifer einen Chiffretext modifizieren könnte, sodass der entschlüsselte Klartext nach wie vor mit dem ursprünglichen Klartext verknüpft ist. Wenn ein Angreifer beispielsweise zwei Bits im Chiffretext spiegelt, würden dieselben Bits im Klartext gespiegelt. CBC wird zudem im Chiffrebasierten-Nachrichtenauthentifizierungscode-Verfahren (CMAC) verwendet, das eine Nachricht gegen Manipulation schützt. Der CMAC wird als sicher angenommen, da es für einen Angreifer wahrscheinlich nicht möglich ist, einen gültigen MAC zu fälschen, ohne den geheimen Schlüssel zu besitzen.

Counter Mode (CTR)

Wie bei CBC wird im CTR-Modus eine zufällige Binärzeichenfolge für jede neue Nachricht ausgewählt, in diesem Fall ein Zähler. Dieser Zähler wird für jeden Nachrichtenblock hochgezählt und verschlüsselt. Die resultierende pseudozufällige Zeichenfolge wird schließlich per XOR-Operation mit der Klartextnachricht verknüpft. Somit wandelt CTR die AES-Blockchiffre faktisch in eine Stromchiffre um. Wenngleich CTR auch die ECB-Schwächen überwindet, leidet auch dieser Modus unter Formbarkeit. Ein weiterer Vorteil von CTR ist seine Fähigkeit, die Verschlüsselung und Entschlüsselung zu beschleunigen, indem die pseudozufällige Zeichenfolge vorberechnet und die XOR-Operationen für die Nachrichtenblöcke parallelisiert werden.

Counter with CBC-MAC (CCM)

Der CCM-Modus kombiniert den CTR-Modus mit einem CBC-MAC, der dem CMAC recht ähnlich ist, aber für Nachrichten variabler Länge nicht als sicher gilt. Somit ist CCM ein kombinierter Verschlüsselungs- und Authentifizierungsblockchiffre-Modus [7] [8].

Wenngleich AES als sicheres Verschlüsselungsverfahren betrachtet wird, hängt sein Sicherheitsniveau auch von seiner Implementierung ab. Fehler bei der Implementierung könnten nach wie vor Schwachstellen in ein eigentlich sicheres kryptografisches Verfahren einführen. Somit kann die Verwendung von AES allein nicht zu dem Schluss führen, dass ein System auf sichere Weise Vertraulichkeit bietet.

AES in LTE-Netzen

In LTE-Netzen können vier Verschlüsselungsalgorithmen für die Kontroll- und Benutzerebene auf der Funkstrecke zum Einsatz kommen: EEA0, EEA1, EEA2 und EEA3 [9] (siehe auch 4.2.2). Während EEA0 für überhaupt keine Verschlüsselung steht, definieren die anderen EEA-Methoden eine symmetrische, synchrone Stromchiffre. Diese gewährleistet eine schnelle Verschlüsselung, da der Chiffrestrom vorberechnet und per XOR-Operation Bit für Bit mit dem Klartext verknüpft werden kann. EEA1 greift auf SNOW 3G (siehe unten) zurück, EEA3 auf den chinesischen Algorithmus ZUC. Der 128-EEA2-Algorithmus basiert auf 128-Bit-AES-Verschlüsselung im CTR-Modus. Die EEA2-Spezifikationen erweitern jedoch die AES-CTR-Methode durch einige zusätzliche Regeln. Sie ist somit komplexer als der ursprüngliche Algorithmus [10].

Dasselbe gilt für den Integritätsalgorithmus 128-EIA2, der verwendet wird, um die Kontroll- und Benutzerebene vor Manipulation zu schützen. Als eine von vier EIA-Optionen basiert EIA2 auf der sicheren 128-Bit-AES-CMAC-Methode.

SNOW 3G

Der LTE-Verschlüsselungsalgorithmus 128-EEA1 sowie der Integritätsalgorithmus 128-EIA1 basieren auf der SNOW-3G-Chiffre [9]. SNOW 3G [11] ist eine wortorientierte Stromchiffre, die vom 3GPP im Jahr 2006 eingeführt und bereits in UMTS verwendet wurde. Der Algorithmus produziert eine pseudozufällige Sequenz von 32-Bit-Wörtern. Diese wird verwendet, um den Klartext zu maskieren.

BEST

Das 3GPP arbeitet an einem speziellen Sicherheitsprotokoll für Geräte mit Energiebeschränkungen, die mit geringem Durchsatz, aber hoher Latenz über LTE- oder 5G-Netzwerke kommunizieren müssen. Diesen Dienst bezeichnet man als Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST) [12]. Die drei wichtigsten Instanzen im BEST-Protokoll sind das Endgerät, der Sicherheitsendpunkt im Netzwerk des Service Providers (HSE) sowie der Anwendungsserver des Unternehmens (EAS). BEST kann in drei Betriebsarten verwendet werden:

- nur für Schlüsselvereinbarung
- für Integritätsschutz
- für Integritäts- und Vertraulichkeitsschutz

Der Integritätsschutzalgorithmus und die Länge des MAC werden vom HSE bei Sitzungsbeginn ausgewählt. Dasselbe gilt für den Verschlüsselungsalgorithmus. Der BEST-Standard greift auf dieselben kryptografischen Mechanismen wie LTE[1] zurück. Bei BEST wird der MAC für eine Nachricht zunächst berechnet und zusammen mit der Payload verschlüsselt, woraufhin er geschützt ist. Die kryptografischen Schlüssel können jederzeit während einer Sitzung aktualisiert werden. Sicherheitsfunktionen stehen für Nachrichten auf der Benutzer- und Kontrollebene zur Verfügung. Nachrichten auf der Kontrollebene werden beim Service Provider beendet. Nachrichten auf der Benutzerebene können hingegen zwischen dem Nutzerendgerät und dem Service Provider (Ende-zu-Mitte) oder zwischen dem Nutzerendgerät und dem Anwendungsserver (Ende-zu-Ende) geschützt werden.

BEST verwendet die bewährten LTE-Netzwerkelemente für Sicherheitszwecke, wie etwa Authentifizierung (siehe 4.2.1), was eine weitere Sicherheitsschicht für LTE-Netze hinzufügt.

[1] Im BEST-Standard wird erwartungsgemäß nur der EEA0-Algorithmus – d. h. keine Verschlüsselung – vom Nutzerendgerät unterstützt. Im Netz der Deutschen Telekom ist jedoch die Verwendung von EE0 untersagt.

3. Sicherheit von LoRaWAN

LoRaWAN definiert eine Systemarchitektur für ein LPWA-Netzwerk sowie ein MAC-Protokoll, das Schicht 2 des OSI-Modells mit einigen Elementen von Schicht 3 entspricht [3]. Als offene Spezifikation, die von der LoRa Alliance definiert wurde, kann LoRaWAN von Telekommunikationsbetreibern für öffentliche Netzwerke sowie von Unternehmen, anderen Organisationen oder Privatpersonen für private Netzwerke verwendet werden. Insbesondere im letzten Fall ist es sehr wichtig, die Sicherheit des LoRaWAN-Netzwerks zu gewährleisten und so Sicher-heitsrisiken durch ignorante oder unvorsichtige Benutzer zu minimie- ren. In den folgenden Abschnitten werden die Sicherheitsimplikationen der physischen LoRaWAN-Schicht und die beiden derzeit verfügbaren LoRaWAN-Architekturversionen beschrieben.

3.1. Modulation: LoRa und Chirp Spread Spectrum

LoRaWAN definiert eine Systemarchitektur für ein LPWA-Netzwerk sowie ein MAC-Protokoll, das Schicht 2 des OSI-Modells mit einigen Elementen von Schicht 3 entspricht [3]. Als proprietäres Protokoll, das von Semtech entwickelt wurde und von der LoRa Alliance unterstützt wird, findet LoRaWAN Verwendung durch Telekommunikationsbetreiber für öffentliche Netzwerke sowie durch Unternehmen, andere Organisationen oder Privatpersonen für private Netzwerke. Insbesondere im letzten Fall ist es sehr wichtig, die Sicherheit des LoRaWAN-Netzwerks zu gewährleisten und so Sicherheitsrisiken durch ignorante oder unvorsichtige Benutzer zu minimieren. In den folgenden Abschnitten werden die Sicherheitsimplikationen der physischen LoRaWAN-Schicht und die beiden derzeit verfügbaren LoRaWAN-Architekturversionen beschrieben.

Electronic Code Book Mode (ECB):
Bevor die Sicherheitsaspekte von LoRaWAN näher beleuchtet werden, ist es wichtig, LoRa (Long Range) von LoRaWAN zu unterscheiden, da die beiden Konzepte fälschlicherweise oft als identisch betrachtet werden. Während LoRaWAN primär die MAC-Schicht eines LPWA-Netzwerks beschreibt, ist LoRa die Modulationstechnologie und somit Teil der physischen Schicht. LoRa ist eine spezielle Modulation, die von dem französischen Unternehmen Cycleo entwickelt wurde, das vom Chiphersteller Semtech übernommen wurde [13]. Folglich wird die Modulation als proprietär betrachtet.

Der zweite Teil der physischen Schicht ist das regionale ISM-Band, die Trägerfrequenzen im jeweiligen Land. LoRa greift auf Sub-1-GHz-Trägerfrequenzen zurück. In Europa kann LoRaWAN die unlizenzierten Trägerfrequenzbänder von 433 MHz und 868 MHz nutzen. Abbildung 2 zeigt die verschiedenen Schichten des Protokollstapels.

Die Nutzung unlizenzierter Frequenzen weist ein Problem auf: Interferenz kann leicht auftreten, insbesondere da jeder diese Frequenzen nutzen kann. Zudem ist die Funkfrequenzstörung (RF-Störung) im unlizenzierten Spektrum einfacher als im lizenzierten Spektrum. Daher basiert LoRa auf einer sehr komplexen Modulationsmethode: Chirp Frequency Spreading (CSS). CSS ist eine Frequenzspreizmethode und wird seit dem Zweiten Weltkrieg eingesetzt. Noch heute wird das Verfahren als sehr robust und relativ schwer abfangbar betrachtet. Chirp-Impulse werden als Symbole übertragen, die im Lauf der Zeit kontinuierlich in der Frequenz steigen oder fallen. Die Datenübertragung wird realisiert, indem diese Chirp-Impulse im Lauf der Zeit aneinandergereiht werden. Aufgrund der Chirp-Impulse verwendet CSS eine große Bandbreite.

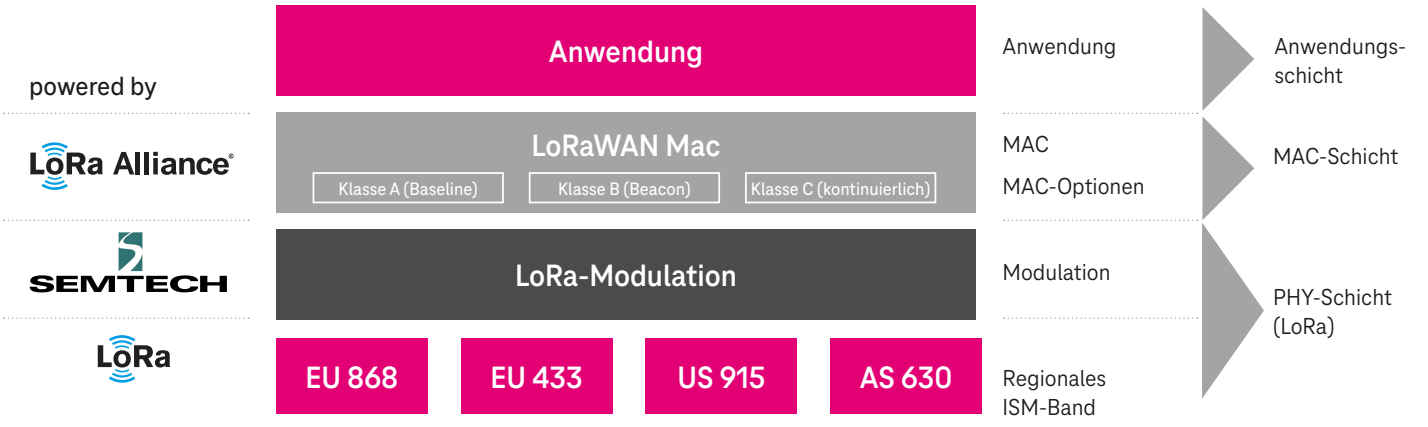


Abbildung 1: Schichtstruktur und Klassifikation von LoRaWAN und LoRa [3]

Ein Vorteil der CSS-Methode liegt in der starken Robustheit gegenüber Schmalbandinterferenz und Störungen, wie etwa dem Dopplereffekt. Zudem bietet CSS ein gewisses Maß an Obskurität: Da die Frequenz kontinuierlich wechselt, kann ein Lauscher Schwierigkeiten haben, komplette Nachrichten abzufangen. Für einen Angreifer kann es sogar schwierig sein zu erkennen, dass eine Übertragung überhaupt stattfindet. Abbildung 3 zeigt den kontinuierlichen Frequenzwechsel während der verschiedenen Felder eines LoRa-Frames. „Sicherheit durch Obskurität" wird jedoch heute nicht als zuverlässiger Ansatz betrachtet und eliminiert daher nicht die Notwendigkeit weiterer Sicherheitsmaßnahmen in den oberen Schichten. Die Nachteile der CSS-Modulation liegen in der hohen Komplexität beim Signalempfang und dem Erfordernis einer großen Bandbreite bei niedrigen Übertragungsfrequenzen (siehe Tabelle 1).

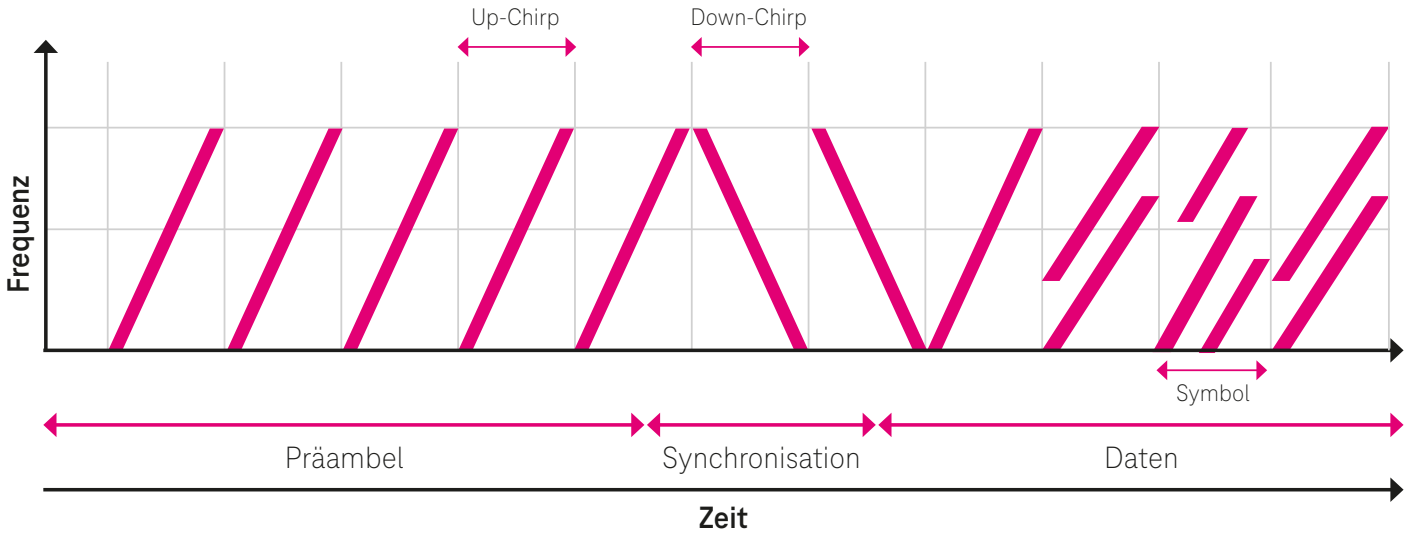


Abbildung 2: Chirp-Spread-Spectrum-Modulation (CSS) [14]

Vorteile und Nachteile von CSS

Vorteile:

- ⊕ **Starke Robustheit** gegenüber Störungen und Interferenzen
- ⊕ **Signalobskurität:** Ein Angreifer kann Nachrichteninhalte ohne Autorisierung nicht zuverlässig abfangen.

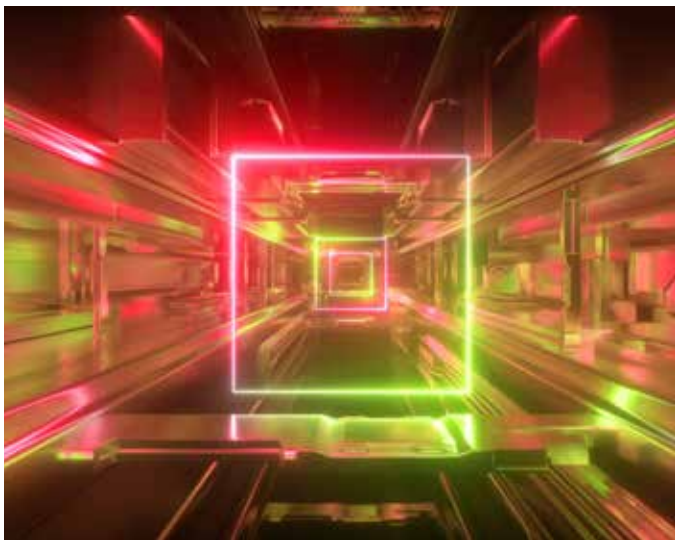
Nachteile:

- ⊖ **RF Störung** ist möglich
- ⊖ **Hohe Komplexität** beim Empfang
- ⊖ **Große Bandbreite** bei niedrigen Übertragungsfrequenzen erforderlich

Tabelle 1: Vorteile und Nachteile des Chirp Spread Spectrum

3.2. LoRaWAN-Architektur v1.0

Die gängigste und derzeit am häufigsten verwendete LoRaWAN-Architektur ist v1.0. Diese Version wurde im Januar 2015 eingeführt. LoRaWAN-Netzwerke weisen eine starke Topologie auf (siehe Abbildung 5). Sie bestehen aus verteilten LoRaWAN-Endgeräten, den Gateways, dem Netzwerkserver und den Anwendungsservern. Für das Endgerät ist es unerheblich, welches Gateway die Datenpakete empfängt und seine Pakete an alle Gateways innerhalb der Reichweite überträgt. Diese leiten die Nachrichten wiederum an den Cloud-basierten Netzwerkserver über eine Backhaul-Technologie weiter (z. B. Eth-ernet). Der Netzwerkserver entfernt Duplikate und sendet die Pakete an den entsprechenden Anwendungsserver. Der Anwendungsserver führt die gewünschte Aktion aus. [3] Obwohl es sich um Anwendungs-daten handelt, können LoRaWAN-Nachrichten verwendet werden, um MAC-Befehle für Netzwerkadministrationszwecke zwischen dem Endgerät und dem Netzwerkserver zu senden [15].



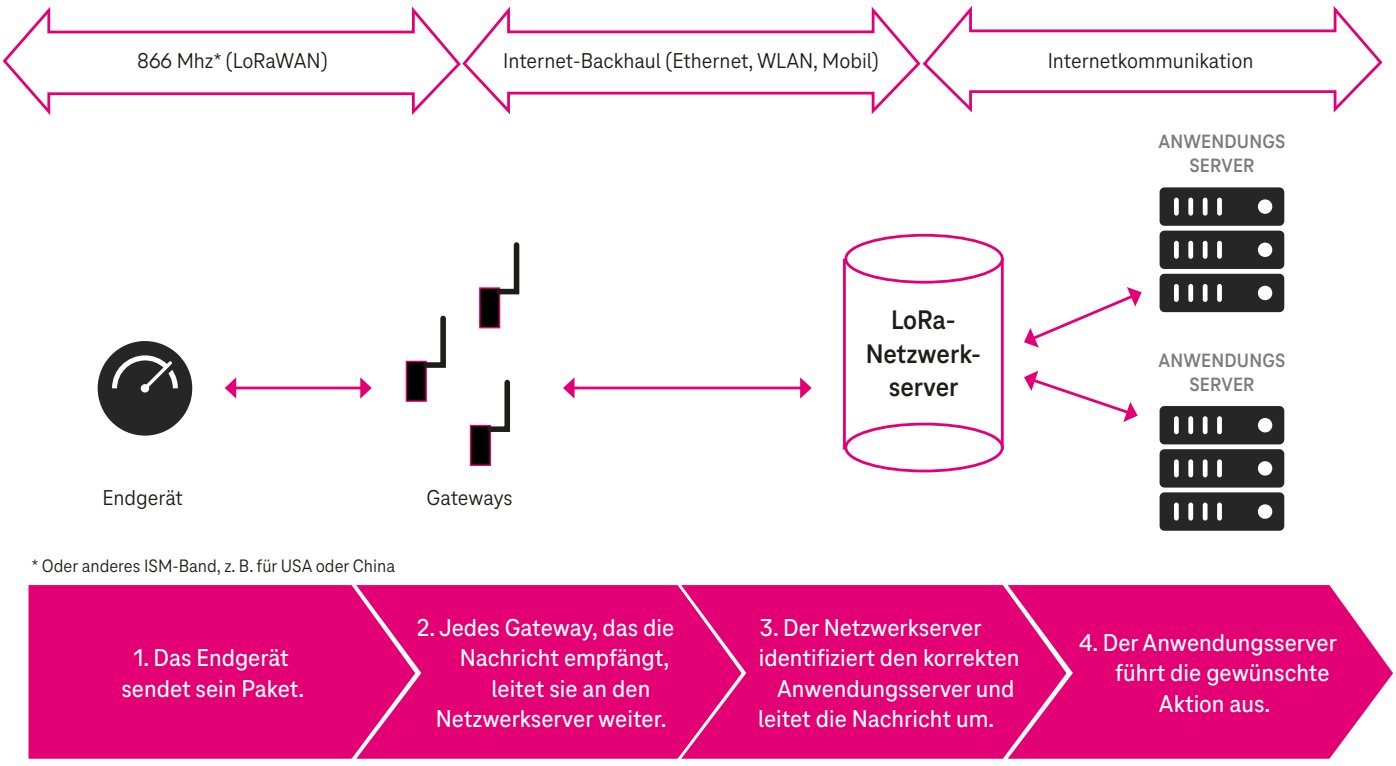


Abbildung 3: LoRaWAN v1.0 Architektur [4]

3.2.1. Verbindungsprozess von LoRaWAN-Endgeräten

Bezeichner und Schlüssel

Um Endgeräte in ein LoRaWAN-v1.0-Netzwerk zu integrieren (Verbindungsprozess), werden verschiedene Schlüssel und Bezeichner benötigt (siehe Tabelle 2). Eine eindeutige Identifizierung wird durch die Bezeichner AppEUI und DevEUI garantiert. Der DevEUI wird dem Gerät vom Gerätehersteller zugewiesen. Der AppEUI muss im Gerät selbst implementiert werden und wird verwendet, um den korrekten Anwendungsserver zu adressieren. Das Gerät benötigt ebenfalls eine Adresse – die DevAddr –, die einmalig im Netzwerk ist.

Bei LoRaWAN v1.0 haben Endgeräte nur einen Hauptschlüssel, den AppKey. Dieser Schlüssel wird vom Gerätehersteller vorkonfiguriert. Um Datenübertragungen zu schützen, sind zwei Sitzungsschlüssel erforderlich: der NwkSKey, der hauptsächlich für die Nachrichtenauthentifizierung verwendet wird, sowie der AppSKey für die Verschlüsselung [15].

Verbindung mit Activation by Personalization (ABP)

Zwei Verbindungsmethoden stehen für LoRaWAN-Endgeräte zur Verfügung. Die einfachere Option bezeichnet man als Activation by Personalization (ABP) (siehe Abbildung 6). ABP wird jedoch nur für Testgeräte empfohlen, da es eine wesentliche Sicherheitsschwachstelle aufweist: Die beiden Sitzungsschlüssel, die für die Nachrichtenverschlüsselung und Authentifizierung verwendet werden, sind dauerhaft im Gerät implementiert. ABP unterstützt nicht das Erstellen neuer Schlüssel. Somit werden Nachrichtenflüsse von einem über ABP verbundenen Gerät – auch aus der Vergangenheit – nur geschützt, solange die Sitzungsschlüssel nicht kompromittiert wurden. ABP bietet damit keine Perfect Forward Secrecy. Zudem könnten Netzwerkadministratoren unsichere Sitzungsschlüssel verwenden oder Schlüssel für verschiedene Geräte wiederverwenden und somit die Angriffsfläche vergrößern. [15]

Verbindung mit Over-The-Air Activation (OTAA)

Die empfohlene Verbindungsmethode im Hinblick auf Sicherheit ist Over-The-Air Activation (OTAA). Bei OTAA empfangen die Geräte ihren eindeutigen Gerätebezeichner (DevEUI) zum Zeitpunkt der Herstellung – den eindeutigen Anwendungsbezeichner (AppEUI) und den Hauptschlüssel (AppKey) jedoch erst bei der Netzwerkregistrierung. Das Verbindungsverfahren besteht aus zwei Nachrichten zwischen dem Gerät und dem Netzwerkserver: der Verbindungsanfrage (Join-Request-Anfrage) und der Join-Accept-Nachricht (siehe Abbildung 4).

Zunächst sendet das Endgerät eine Verbindungsanfrage an den Netzwerkserver, die die beiden Bezeichner AppEUI und DevEUI enthält. Zudem wird eine zufällige Nonce gesendet, um vor Replay-Angriffen zu schützen, bei denen ein Angreifer eine frühere Verbindungsan-frage erneut sendet. [15] Untersuchungen haben jedoch gezeigt, dass dieser Mechanismus nicht ausreicht: Es konnte verhindert werden, dass sich ein Endgerät mit dem Netzwerk verbindet, indem der Zufallszahlengenerator so manipuliert wurde, dass er eine Nonce innerhalb eines bestimmten Zeitraums erneut verwendet [16]. Die Verbindungsanfrage wird nicht verschlüsselt, aber mithilfe von AES-128-CMAC integritätsgeschützt. Das Endgerät verwendet den vorkonfigurierten Hauptschlüssel AppKey, um einen MIC für die komplette Nachricht zu berechnen. Somit authentifiziert es sich zudem implizit, indem es den Besitz des geheimen Hauptschlüssels nachweist.

Der Netzwerkserver validiert den MIC mithilfe des AppKeys, der für das Gerät gespeichert wurde. Außerdem prüft er die Nonce anhand einer begrenzten Liste mit Noncen, die von dem Endgerät in der Vergangenheit verwendet wurden. Schließlich sendet der Server eine Join-Accept-Nachricht an das Endgerät und übermittelt die Geräteadresse (DevAddr), einen Netzwerkbezeichner (NetID) und eine weitere Nonce. Die gesamte Nachricht wird zunächst mit einer AES-128-Entschlüsselungsoperation im ECB-Modus verschlüsselt. Die Wahl des ECB-Modus ist jedoch etwas eigenartig, da diese Betriebsart bekannt dafür ist, dass sie Muster in verschlüsselten Daten verhindert (wie in Kapitel 2 beschrieben). Die verschlüsselte Join-Accept-Nachricht wird durch einen MIC geschützt, der mit dem AppKey berechnet wurde.

Endgerät und Netzwerkserver berechnen daraufhin die Sitzungsschlüssel: NwkSKey und AssSKey. Dies erfolgt durch Verschlüsselung einer Zeichenfolge, die den Netzwerkbezeichner und die Noncen enthält, unter Verwendung von AES-128 und dem AppKey [15]. Die Verwendung eines Hauptschlüssels für die Ableitung der geheimen Schlüssel für Integritäts- und Vertraulichkeitsschutz wird jedoch vom Sicherheitsstandpunkt aus nicht empfohlen. Der Netzwerkserver überträgt den AppSKey an den Anwendungsserver, nachdem der Verbindungsprozess abgeschlossen wurde, und soll diesen Sitzungsschlüssel daraufhin löschen [17]. Wenn das Mobilgerät die Schlüssel oder die Verbindung zum Netzwerk verliert, oder wenn das Netzwerk die Gültigkeit der Schlüssel beendet, muss das Mobilgerät ein neues Verbindungsverfahren einleiten.

Fazit

Jeder, der ein LoRaWAN-Netzwerk betreibt oder nutzt, sollte grundsätzlich die OTAA-Methode anwenden. Diese Methode ist bei Weitem die sicherste Verbindungsmethode für LoRaWAN-Netzwerke im Standardbetrieb. Um dies nochmals zu verdeutlichen, werden die beiden Anmeldungs- und Authentifizierungsprozesse in Tabelle 2 verglichen.

LoRaWAN v1.0				
Schlüssel	Beschreibung	Erforderlich für Verbindungstyp		Generierung
		OTAA	ABP	
Benötigte Schlüssel vor Aktivierung				
AppKey	Wird verwendet, um AppSKey und NwkSKey abzuleiten und das OTAA-Verbindungsverfahren zu sichern.	Ja	Nein	Vorab gespeichert
Benötigte Schlüssel nach Aktivierung				
NwkSKey	Wird verwendet, um MICs zu berechnen/verifizieren und um reine MAC-Pakete zu verschlüsseln	Ja	Ja	ABP: manuell generiert OTAA: generiert aus AppKey und Join-Accept-Nachricht
AppSKey	Wird verwendet, um die Payload der Datenpakete zu verschlüsseln/entschlüsseln	Ja	Ja	ABP: manuell generiert OTAA: generiert aus AppKey und Join-Accept-Nachricht
Bezeichner				
AppEUI	Global eindeutiger 64-Bit-Anwendungsbezeichner	Ja	Nein	Vorab gespeichert
DevEUI	Global eindeutiger 64-Bit-Gerätebezeichner, der vom Netzwerkserver zugewiesen wird	Ja	Nein	Vorab gespeichert
DevAddr	Eindeutige 32-Bit-Geräteadresse im aktuellen Netzwerk	Ja	Ja	ABP: manuell generiert OTAA: empfangen durch Join-Accept-Nachricht

Tabelle 2: Sicherheitsschlüssel und Bezeichner in einer LoRaWAN-Architektur v1.0 [15]

Abbildung 4: OTAA-Registrierungsprozess eines LoRaWAN-Geräts [9]

Activation by Personalization (ABP)

Vorteile:

- ⊕ **Vereinfachter** Inbetriebnahme-Prozess
- ⊕ **Schnell:** Geräte sind umgehend funktionsfähig

Nachteile:

- ⊖ **Manuelle Generierung der Sitzungsschlüssel** könnte zu wiederverwendeten oder unsicheren Schlüsseln führen
- ⊖ **Keine Schlüsselerneuerung**

Over-the-Air Activation (OTAA)

Vorteile:

- ⊕ **Integritäts- und Vertraulichkeitsschutz** für Verbindungsnachrichten
- ⊕ **Implizite gegenseitige Authentifizierung** durch Nachweis des Besitzes des Hauptschlüssels
- ⊕ **Sichere Schlüsselgenerierung** mit AES-128, Noncen und dem Hauptschlüssel
- ⊕ **Erstellen neuer Sitzungsschlüssel** ist möglich

Nachteile:

- ⊖ **AES im nicht empfohlenen ECB-Modus** wird für Verschlüsselung verwendet
- ⊖ **Notwendigkeit verbesserter Schlüsselgenerierung**, da der Hauptschlüssel für beide Sitzungsschlüssel verwendet wird

Tabelle 3: Vorteile und Nachteile der LoRaWAN-v1.0-Verbindungsmethoden

3.2.2. Daten-übertragung

LoRaWAN-Frames bestehen aus fünf Feldern, wie in Tabelle 4 beschrieben. Jede Nachricht wird durch einen MIC integritätsgeschützt, der über alle Felder des MAC-Frames, einschließlich Header und Payload, berechnet wird. Wie bei OTAA werden AES-128-CMAC und der NwkSKey für die MIC-Berechnung verwendet. Wenn die Payload (FRMPayload) jedoch nicht leer ist, muss das FRMPayload-Feld vor der MIC-Berechnung verschlüsselt werden. Das verwendete Verschlüsselungsverfahren ist AES-128 im CCM-Modus, einer Erweiterung des CCM-Modus. Für die Verschlüsselung von Anwendungsdaten wird der AppSKey ausgewählt. [15] [8]

Frames, die MAC-Befehle umfassen, sind somit nur zwischen dem Endgerät und dem Netzwerkserver Ende-zu-Ende integritäts- und vertraulichkeitsgeschützt (siehe **Tabelle 5**). Frames, die Anwendungsdaten umfassen, werden zwischen dem Endgerät und dem Anwendungsserver Ende-zu-Ende verschlüsselt. Während des OTAA-Verbindungsprozesses ist der Netzwerkserver dennoch im Besitz des AppSKey und könnte Anwendungsdaten entschlüsseln, wenn der Schlüssel nicht gelöscht wird, wie durch die LoRaWAN-Spezifikation vorgesehen. Zudem ist die Integrität nur zwischen dem Endgerät und dem Netzwerkserver gewährleistet. Somit könnten Anwendungspayloads durch einen Netzwerkserver oder während der Übertragung zum Anwendungsserver manipuliert werden. Dies ist darauf zurückzuführen, dass in der LoRaWAN-v1.0-Spezifikation Netzwerkdienste als vertrau-enswürdige Parteien betrachtet werden. Um diese Sicherheitslücke zu schließen, sollten LoRaWAN-Netzwerkbetreiber zusätzliche Sicher-heitsmaßnahmen implementieren, wie etwa VPN zwischen Netzwerk-server und Anwendungsserver. [15]

MHDR	FHDR
MAC header	Frame header
Integritätsgeschützt	Integritätsgeschützt
FPort	**FRMPayload**
Optional, spezifiziert den Typ der FRMPayload	Playload mit MAC-Befehlen und/oder Anwendungsdaten
Integritätsgeschützt	Integritätsgeschützt und verschlüsselt
MIC	
Message integrity code	

Tabelle 4: Frame-Format einer LoRaWAN-Datennachricht [15]

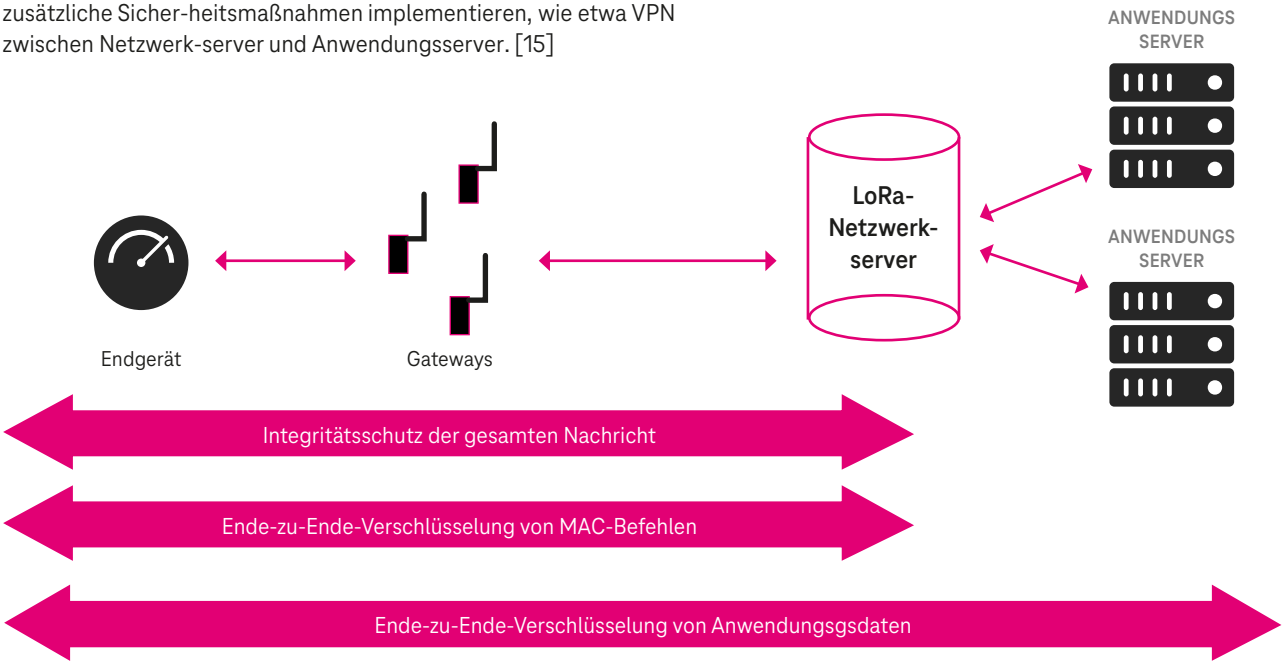


Abbildung 5: Sicherheit von LoRaWAN-Datennachrichten

Vorteile:

⊕ **Integritätsschutz** für alle Frame-Felder
⊕ **Ende-zu-Ende-Verschlüsselung** für Anwendungsdaten und MAC-Befehle

Nachteile:

⊖ **Integritätsschutz für Anwendungsdaten** nur zwischen dem Endgerät und dem Netzwerkserver
⊖ **Schwachstelle in der Ende-zu-Ende-Verschlüsselung** für Anwendungsdaten, da der Netzwerkserver den Verschlüsselungsschlüssel besitzt

Tabelle 5: Vorteile und Nachteile der LoRaWAN-v1.0-Datenübertragung

Wissenschaftliche Untersuchungen haben gezeigt, dass die LoRaWAN-Architektur v1.0 mehrere Sicherheitsschwachstellen mit unterschiedlichem Schweregrad aufweist. Einige wurden bereits in den vorstehenden Abschnitten erwähnt. Die folgenden LoRaWAN-v1.0-Schwachstellen sind hinreichend bekannt.

LoRaWAN-Endpunkte enthalten einen Hauptschlüssel, der sich während ihrer Lebensdauer nicht ändert und auch für das gesamte Netzwerk verwendet werden kann. Kompromittierte Schlüssel geben somit vergangene und aktuelle Nachrichten preis – potenziell im gesamten Netzwerk. Zudem ist Kosteneffizienz eines der wichtigsten Kriterien für diese Geräte. Daher umfassen LoRaWAN-Geräte häufig kein sicheres Element, das kryptografische Informationen auf sichere Weise speichert. Angreifer könnten somit Erfolg bei der Extraktion von Schlüsseln von einem Endgerät, das in ihren Besitz gelangt, oder bei der Einführung von Schadfirmware haben. Eine Beschränkung der Ende-zu-Ende-Verschlüsselung von Anwendungsdaten liegt darin, dass der Netzwerkserver ursprünglich den Anwendungsschlüssel AppSKey kennt (wie in 3.2.1 beschrieben) [17]. Es steht nicht fest, ob der AppSKey vom Netzwerkserver nach dem Verbindungsprozess sicher gelöscht wird.

Die meisten LoRaWAN-Geräte sind nur gelegentlich mit dem Netzwerk verbunden. Dieser Umstand kann genutzt werden, um physische Hacks einfacher durchzuführen, ohne sofort bemerkt zu werden. Ein weiterer Aspekt, der Aufmerksamkeit erfordert, ist, dass LoRaWAN keine Integrität zwischen Netzwerk- und Anwendungsserver gewährleistet und den Hauptschlüssel als Basis für die beiden Sitzungsschlüssel verwendet. Im Fall einer möglichen Kompromittierung kann es äußerst schwierig sein, einen sicheren Zustand für ein LoRaWAN-Netzwerk widerherzustellen: Der AppKey muss für jedes Gerät geändert werden. Bei vielen Geräten erweist sich diese Maßnahme als sehr kostenintensiv und komplex.

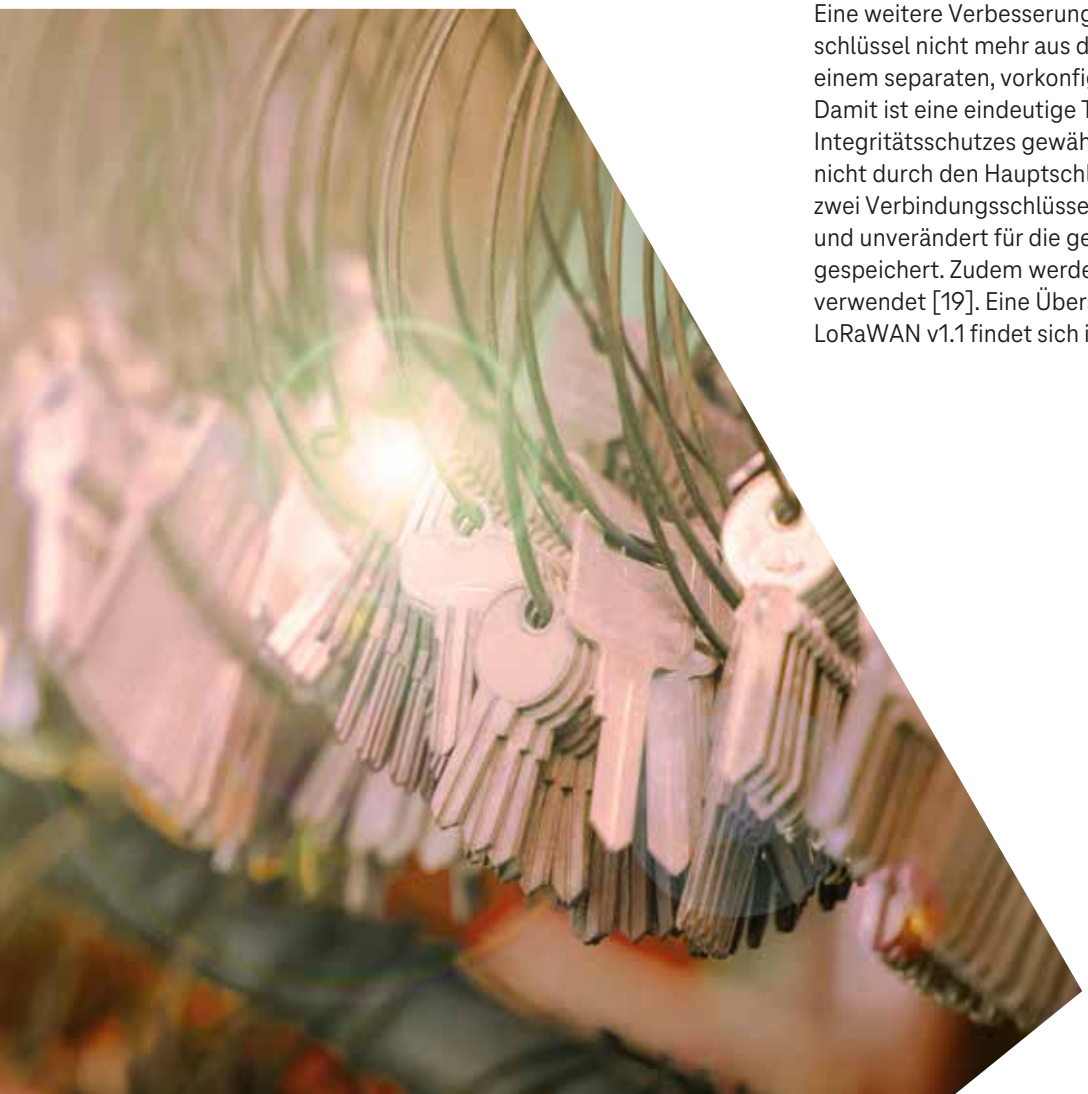
Diese Sicherheitsschwachstellen werden u. a. genutzt, um bestimmte Angriffe durchzuführen. Tabelle 6 enthält eine Übersicht zu Angriffen, die möglich sind. Die beiden Angriffe mit der vermeintlich größten Auswirkung sind physische Gateway-Angriffe und bösartige Gateway-Angriffe. Beide gehen davon aus, dass ein Angreifer Zugriff auf ein oder mehrere LoRaWAN-Gateway(s) erhält. Bei einem physischen Gateway-Angriff könnte der Angreifer die Gateways deaktivieren und damit das Netzwerk lahmlegen. Bei einem bösartigen Gateway-Angriff könnten Sensordaten zu einem schädlichen Netzwerkserver umgeleitet werden. In der Folge kann der Angreifer versuchen, Nachrichten zu manipulieren. [18]

Angriff	Kosten	Know-how	Ergebnis	Erkennbarkeit	Vermeidbarkeit	Potenzielle Auswirkung
Zählerüberlauf Einführung von Nachrichten mit Frame-Zähler 0, damit gültige Nachrichten ignoriert werden (nur mit ABP)	niedrig	hoch	Fake-Nachrichten	mittel	einfach	gering
Physischer Gateway-Angriff Deaktivierung von Gateways, um das Netzwerk zu verlangsamen oder lahmzulegen	niedrig	mittel	cripple networks	einfach	mittel	**hoch**
Bösartiger Gateway-Angriff Manipulation von Gateways, um Nachrichten an einen Fake-Netzwerkserver umzuleiten	mittel	hoch	Fake-Nachrichten	schwierig	mittel	**hoch**
Physischer Sensorangriff Abfangen von Sensordaten aus der Kommunikation zwischen zwei Chips in einem Endgerät	mittel	mittel	Fake-Nachrichten	schwierig	difficult	gering
Generische Störung Senden auf denselben Frequenzen, um die Übertragung aller Pakete zu stören	hoch	niedrig	Lahmlegung von Netzwerken	einfach	difficult	gering
Selektive Störung Senden auf denselben Frequenzen, um die Übertragung eines speziellen Pakets zu stören	hoch	hoch	Fake-Nachrichten	schwierig	mittel	gering
Replay-Angriff Erneutes Senden einer ursprünglich gesendeten Nachricht	niedrig	hoch	Fake-Nachrichten	schwierig	einfach	gering
Wurmloch-Angriff Stoppen des Empfangs einer Nachricht durch einen Störangriff und daraufhin erneutes Senden der Nachricht	hoch	hoch	Fake-Nachrichten	schwierig	mittel	gering

Tabelle 6: Untersuchung von Angriffen und ihrer Auswirkung auf eine LoRaWAN-Architektur v1.0 [18]

3.3. LoRaWAN Architektur v1.1

Der LoRa Alliance sind die Schwächen, die unter 3.2.3 angesprochen wurden, bekannt. Aus diesem Grunde wurde die neue LoRaWAN-Architektur im Oktober 2017 eingeführt. Bis heute (September 2020) gibt es aber nach wie vor keinen bekannten Anbieter, der die LoRaWAN-v1.1-Architektur in großem Maßstab eingeführt hat. Einige kritische Schwachstellen wurden jedoch mit der neuen Architektur geschlossen, und sie wird wahrscheinlich in der Zukunft größere Verbreitung finden. Daher wird die Architek-tur v1.1 hier ebenfalls berücksichtigt.



Die größten Änderungen gegenüber LoRaWAN v1.0 sind drei Server, die in die Architektur einbezogen wurden (siehe Abbildung 6):

- Ein Verbindungsserver: Der Verbindungsserver übernimmt die Verwaltung des OTAA-Verbindungsprozesses vom Netzwerkserver. Dieser ist für die Generierung der Sitzungsschlüssel zuständig. Während der Netzwerksitzungsschlüssel daraufhin an den Netzwerkserver gesendet wird, erlangt dieser zu keinem Zeitpunkt den Besitz des AppSKey, der für die Verschlüsselung von Anwendungsdaten verwendet wird. Somit wird eine echte Ende-zu-Ende-Verschlüsselung auf Anwendungsebene realisiert.

- Zwei weitere Netzwerkserver für die Bedienung und Weiterleitung: Diese ermöglichen das Roaming von Paketen in fremde LoRaWAN-Netzwerke.

Eine weitere Verbesserung liegt darin, dass der Netzwerksitzungsschlüssel nicht mehr aus dem AppKey generiert wird, sondern aus einem separaten, vorkonfigurierten Hauptschlüssel (NwkKey). Damit ist eine eindeutige Trennung des Vertraulichkeits- und Integritätsschutzes gewährleistet. Der Verbindungsprozess wird nicht durch den Hauptschlüssel gesichert, sondern es werden zwei Verbindungsschlüssel aus den Hauptschlüsseln generiert und unverändert für die gesamte Lebensdauer des Geräts gespeichert. Zudem werden vier statt zwei Sitzungsschlüssel verwendet [19]. Eine Übersicht über die relevanten Schlüssel für LoRaWAN v1.1 findet sich in Tabelle 7.

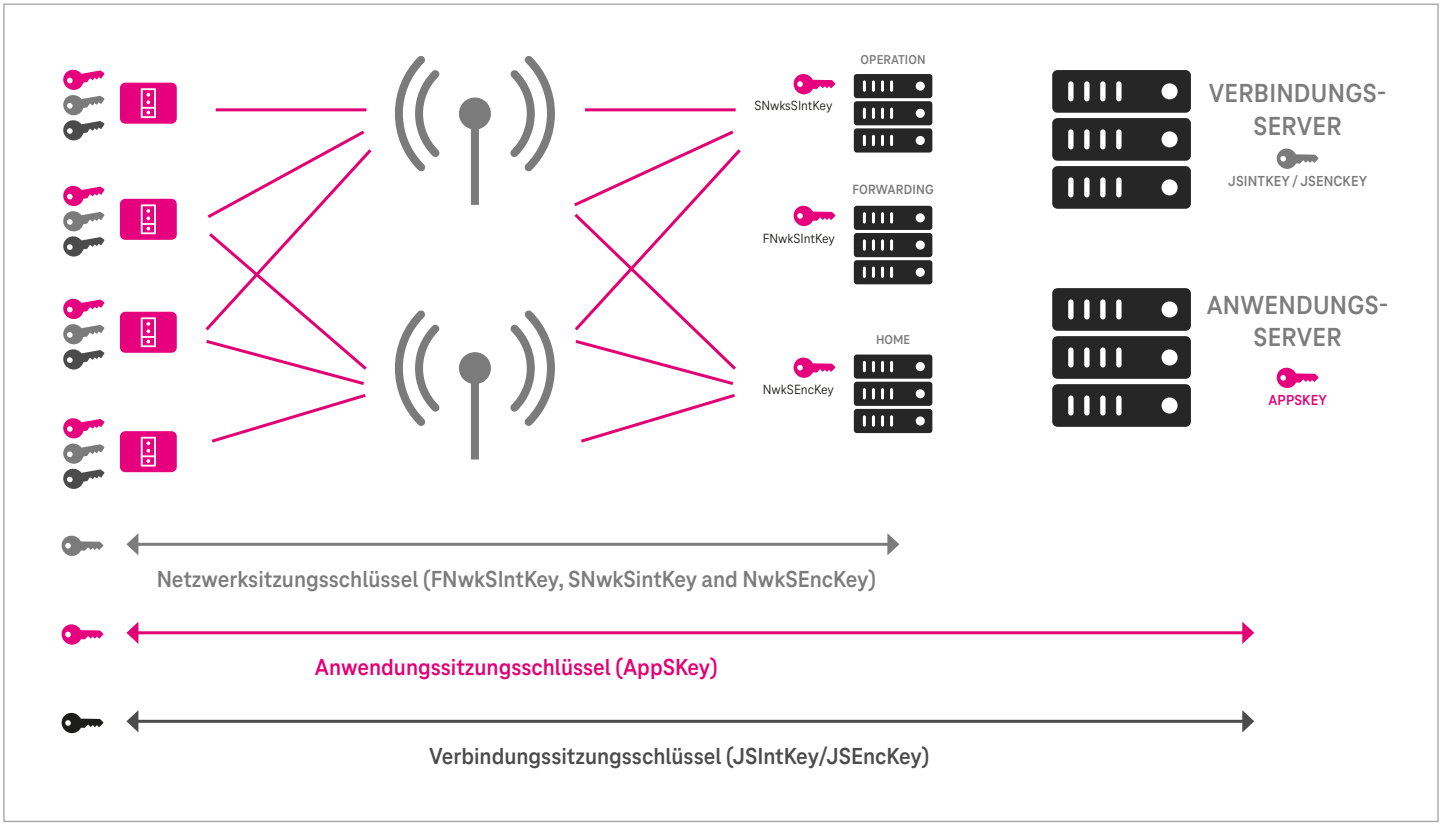


Abbildung 6: LoRaWAN-Architektur v1.1 (Release 2017) [16]

LoRaWAN v1.1				
Schlüssel	Beschreibung	Erforderlich für Verbindungstyp		Generierung
		OTAA	ABP	
Benötigte Schlüssel vor Aktivierung				
NwkKey	Wird für den MIC für Verbindungsanfragepakete verwendet, um Verbindungsannahmepakete zu verschlüsseln und alle Netzwerksitzungsschlüssel abzuleiten.	Ja	Nein	Vorab gespeichert
AppKey	Wird verwendet, um den AppSKey abzuleiten	Ja	Nein	Vorab gespeichert
JSIntKey	Wird für den MIC von erneuten Verbindungsanfrage- und Verbindungsannahmepaketen verwendet	Ja	Nein	OTAA: generiert aus NwkKey und DevEUI
JSEncKey	Wird verwendet, um eine Verbindungsannahme zu verschlüsseln, die durch eine erneute Verbindungsanfrage ausgelöst wird	Ja	Nein	OTAA: generiert aus NwkKey und DevEUI
Benötigte Schlüssel nach Aktivierung				
FNwkSIntKey	Wird als Teil des MIC für Uplink-Datenpakete verwendet	Ja	Ja	ABP: manuell generiert OTAA: Generiert aus NwkKey und Verbindungsannahmenachricht
SNwkSIntKey	Wird für den MIC aller Downlink-Datenpakete sowie für einen Teil des MIC für Uplink-Pakete verwendet	Ja	Ja	ABP: manuell generiert OTAA: Generiert aus NwkKey und Verbindungsannahmenachricht
NwkSEncKey	Wird verwendet, um alle Downlink- und Uplink-MAC-Pakete zu verschlüsseln	Ja	Ja	ABP: manuell generiert OTAA: Generiert aus NwkKey und Verbindungsannahmenachricht
AppSKey	Wird verwendet, um die Payload der Datenpakete zu verschlüsseln/entschlüsseln	Ja	Ja	ABP: manuell generiert OTAA: Generiert aus NwkKey und Verbindungsannahmenachricht
Bezeichner				
JoinEUI	Global eindeutiger 64-Bit-Anwendungsbezeichner, der den Verbindungsserver identifiziert	Ja	Nein	Vorab gespeichert
DevEUI	Global eindeutiger 64-Bit-Gerätebezeichner, der vom Netzwerkserver zugewiesen wird	Ja	Nein	Vorab gespeichert
DevAddr	Eindeutige 32-Bit-Geräteadresse im aktuellen Netzwerk	Ja	Ja	ABP: manuell generiert OTAA: empfangen durch Verbindungsannahmenachricht

Tabelle 7: Sicherheitsschlüssel und Bezeichner in einer LoRaWAN-Architektur v1.1 [20]

3.3.1 Schwachstellen von LoRaWAN v1.1

Viele kritische Schwachstellen der LoRaWAN-Architektur v1.0 wurden in v1.1 behoben. Aber die neue Architektur ist nicht frei von Schwachstellen oder Sicherheitsrisiken. Eine der Hauptschwächen sind nach wie vor die Endpunkte: Ihre Firmware kann verändert und das Gerät damit manipuliert werden. Zudem könnte ein Angreifer geheime Schlüssel erfolgreich aus einem Gerät extrahieren, da viele Gerätehersteller aufgrund der hohen Preise nach wie vor keine Sicherheitselemente implementieren. Wissenschaftliche Untersuchungen zur Architektur v1.1 haben jedoch weitere Sicherheitsrisiken ergeben. Beispielsweise wird die Verbindungsannahmenachricht weiterhin mit AES-128 im nicht empfohlenen ECB-Modus verschlüsselt. Was noch schlimmer ist: Anders als in v1.0 erfordert die Schlüsselgenerierung jetzt eben-falls die Verwendung einer Betriebsart und greift auf den ECB-Modus zurück [19]. Butun et al. [16] haben hervorgehoben, dass das Erstellen neuer Hauptschlüssel nach wie vor nicht möglich ist. Sie haben zudem verschiedene mögliche Angriffe[2] beurteilt und die folgenden Angriffe als diejenigen mit dem höchsten Risiko in einer der vier Kategorien Vertraulichkeit, Integrität, Verfügbarkeit sowie Authentifizierungs- und Zugriffskontrolle identifiziert:

- **Klonen von Geräten oder Austauschen der Firmware:** Ein Angreifer mit physischem Zugriff auf ein LoRaWAN-Gerät könnte die Firmware flashen oder Schlüssel extrahieren. Da ein solcher Angriff einfach durchzuführen, schwer festzustellen und wahrscheinlich äußerst attraktiv für Cyberkriminelle ist, wird das Risiko bei der Authentifizierungs- und Zugriffskontrolle als kritisch hoch betrachtet.

- **Self-Replay-Angriff:** Ein Angreifer beobachtet eine Verbindungsanfragenachricht und unterbricht die Übertragung der entsprechenden Verbindungsannahmenachricht durch RF-Störung. Nach einem Timeout sendet das Gerät die Verbindungsanfrage erneut, und die Antwort wird wiederum verhindert. Dieser Angriff verringert damit die Verfügbarkeit des Netzwerks.

- **Bösartiger Endpunktangriff:** Ein Angreifer führt ein authentisch aussehendes, aber bösartiges Endgerät in ein LoRaWAN-Netzwerk ein, beispielsweise durch Wiederverwendung von Schlüsselmaterial, das aus einem gültigen Gerät extrahiert wurde. Das bösartige Gerät wird verwendet, um das Netzwerk zu stören, falsche Daten in den Anwendungsserver einzuführen oder Pakete erneut zu senden und damit die Gateway-Verfügbarkeit zu verringern. Insbesondere das Risiko für die Authentifizierungs- und Zugriffskontrolle wird als kritisch hoch betrachtet.

[2] Die detaillierte Risikoanalyse zu möglichen LoRaWAN-v1.1-Angriffen findet sich in [16].

4. Sicherheit von NB-IoT

Narrowband-IoT (NB-IoT) ist eine IoT-Funktechnologie, die im lizenzierten Spektrum betrieben wird. Wie der Name vermuten lässt, verwendet NB-IoT Schmalbandfrequenzen. Diese können genutzt werden, weil alle nicht benötigten LTE-Funktionen (z. B. Sprachübertragung) entfernt wurden. Somit sind Datenpakete so klein wie möglich, und ein geringer Energieverbrauch ist realisierbar. NB-IoT basiert auf dem LTE-Standard und profitiert damit von den getesteten und bewährten Sicherheitsmechanismen von LTE. Diese werden durch Standardisierung seitens 3GPP sichergestellt.

4.1. Modulation: OFDMA/ SC-FDMA

NB-IoT nutzt das GSM- oder LTE-Frequenzspektrum [1]. Die Modulationstechnologie unterscheidet sich für Uplink und Downlink. Downlink-Übertragungen greifen auf Orthogonal Frequency Division Multiplex Access (OFDMA) auf der Basis von Quadrature Amplitude Modulation mit 64 verschiedenen Symbolen (64QAM) zurück. OFDMA unterteilt das verfügbare Frequenzband in eine Vielzahl kleiner Subkanäle. Die zu übertragenden Daten werden dann in verschiedene Datenströme aufgeteilt, die parallel über die Subkanäle übertragen werden. Die Verwendung vieler Subträger macht die OFDM-Methode sehr robust, da Störungen auf speziellen Frequenzen nicht den kompletten Datenstrom betreffen [21]. Die 64QAM-Modulation bietet 64 Signalzustände, die aus verschiedenen Kombinationen aus Amplitude und Phase bestehen. Dies ermöglicht die Übertragung von 6 Bits pro Symbol und unterstützt somit höhere Datenraten als niederwertigere Modulationsverfahren wie 16QAM. Für Uplink-Übertragungen verwendet NB-IoT Single-Carrier Frequency Division Multiple Access (SC-FDMA) mit 64QAM, da diese Methode energieeffizienter ist und somit die Lebensdauer des Akkus in den Endgeräten verlängert. Wenngleich SC-FDMA von ODFMA abgeleitet wurde, verwendet das Verfahren nur einen Träger, anstelle der Parallelübertragung von Datensymbolen, und jedes Datensymbol wird über das verfügbare Spektrum gespreizt [22].

Die physische Schicht von LTE und damit von NB-IoT wird durch die 3GPP-Standards ausführlich beschrieben. Sie ermöglicht potenziellen Angreifern beispielsweise Angriffe wie RF-Störung für (siehe auch [23]). Zudem ist es heute – aufgrund der Verfügbarkeit von softwaredefinierten Radios, Open-Source-Software und preiswerten Antennen – relativ einfach und kostengünstig, eine böswillige Basisstation für LTE einzurichten und LTE-Signale zu empfangen. LTE-Netze wenden jedoch gegenseitige Authentifizierung zwischen Endgeräten und Basisstationen an (wie in Abschnitt 4.2.1 unten beschrieben) und sind somit nicht so anfällig für Angriffe von Fake-Basisstationen wie GSM.

Vorteile:

- ⊕ **Robustheit** gegenüber Störungen
- ⊕ Ideal für Anwendungen mit geringer Bandbreite, führt zu reduzierter Latenz und erhöhter Effizienz.
- ⊕ Aufgrund der gegenseitigen Authentifizierung ist es schwierig, falsche Basisstationen in das Netzwerk zu integrieren.

Nachteile:

- ⊖ **RF Störung** ist möglich
- ⊖ **Fake-Basisstationen** sind einfach zu erzeugen, aber aufgrund der gegenseitigen Authentifizierung schwer in ein Netzwerk zu integrieren

Tabelle 8: Vorteile und Nachteile von OFDMA/SC-FDMA

4.2. NB-IoT-Architektur

Die NB-IoT-Architektur basiert auf der LTE-Architektur. Die Gesamtarchitektur des zugrunde liegenden LTE-Systems bezeichnet man als Evolved Packet System (EPS). Das EPS ist ein IP-basiertes Netzwerk mit eindeutig definierten Schnittstellen. Es wurde mit dem ersten LTE-Standard (3GPP Release 8) im Dezember 2008 eingeführt und seitdem ständig erweitert. Abbildung 12 zeigt die für NB-IoT relevanten EPS-Komponenten. Diese Architektur wird auch als das 3GPP-Cellular-IoT-Netzwerk (CIoT-Netzwerk) bezeichnet.

Das Nutzerendgerät (User Equipment, UE) besteht aus einem Endgerät – in diesem Fall ein NB-IoT-Gerät – und einer SIM-Karte (einschließlich der UICC-Hardware und der USIM-Anwendung). Das UE verbindet sich mit der Basisstation (eNodeB) über die LTE-Uu-Funkschnittstelle. Die Daten der Benutzerebene werden dann über die S1-U-Schnittstelle an das Serving Gateway (SGW) des EPC übertragen. Benutzerdaten, die über die Benutzerebene übertragen wurden, werden vom Packet Data Network Gateway (PGW) zum CIoT-Anwendungsserver geleitet. Die Daten der Kontrollebene werden zur Mobility Management Entity (MME) über die S1-MME-Schnittstelle übertragen. In Abhängigkeit vom Anbieter können die Funktionen der Knoten der Kontrollebene (MME) und der Knoten der Benutzerebene (SGW, PGW) in einer Komponente mit der Bezeichnung C-SGN (CIoT Serving Gateway Node) zusammengefasst werden. Wenn Benutzerdaten über die Kontrollebene übertragen werden, ermöglicht die Service Capability Exposure Function (SCEF) (sofern im Kernnetzwerk implementiert) eine RESTfulAPI für die Übertragung der Payload. Die Datenübertragung für den Downlink wird umgekehrt durchgeführt.

Eine Unterscheidung in den 3GPP-Spezifikationen ist besonders wichtig, um das Sicherheitskonzept von NB-IoT zu verstehen. Die Cellular-Protokolle werden in die Zugriffsschicht (Access Stratum, AS) und die Nichtzugriffsschicht (Non-Access Stratum, NAS) unterteilt:

- Die AS umfasst alle Protokolle für die Kommunikation zwischen UE und eNodeB über die Funkschnittstelle. Daher enthält sie Protokolle für die Benutzer- und Kontrollebene.
- Die NAS umfasst den gesamten funkunabhängigen Signalübertragungsverkehr zwischen UE und MME und entspricht lediglich Protokollen der Kontrollebene [24].

Protokolle der Kontrollebene werden normalerweise ausschließlich für Signalübertragungs- und Kontrollaufgaben verwendet. Die Übertragung kleiner Datenmengen über die Benutzerebene kann jedoch ineffizient sein. Daher ermöglicht NB-IoT auch die Übertragung kleiner Datenmengen über die Kontrollebene – mit oder ohne TCP/IP-Header. Diese Technologie wird als Data over NAS bezeichnet [25].

Mobility Management Entity (MME)

⊕ Authentifizierung & Autorisierung des
⊕ Non-Access-Stratum-Protokolls (NAS-Schicht)

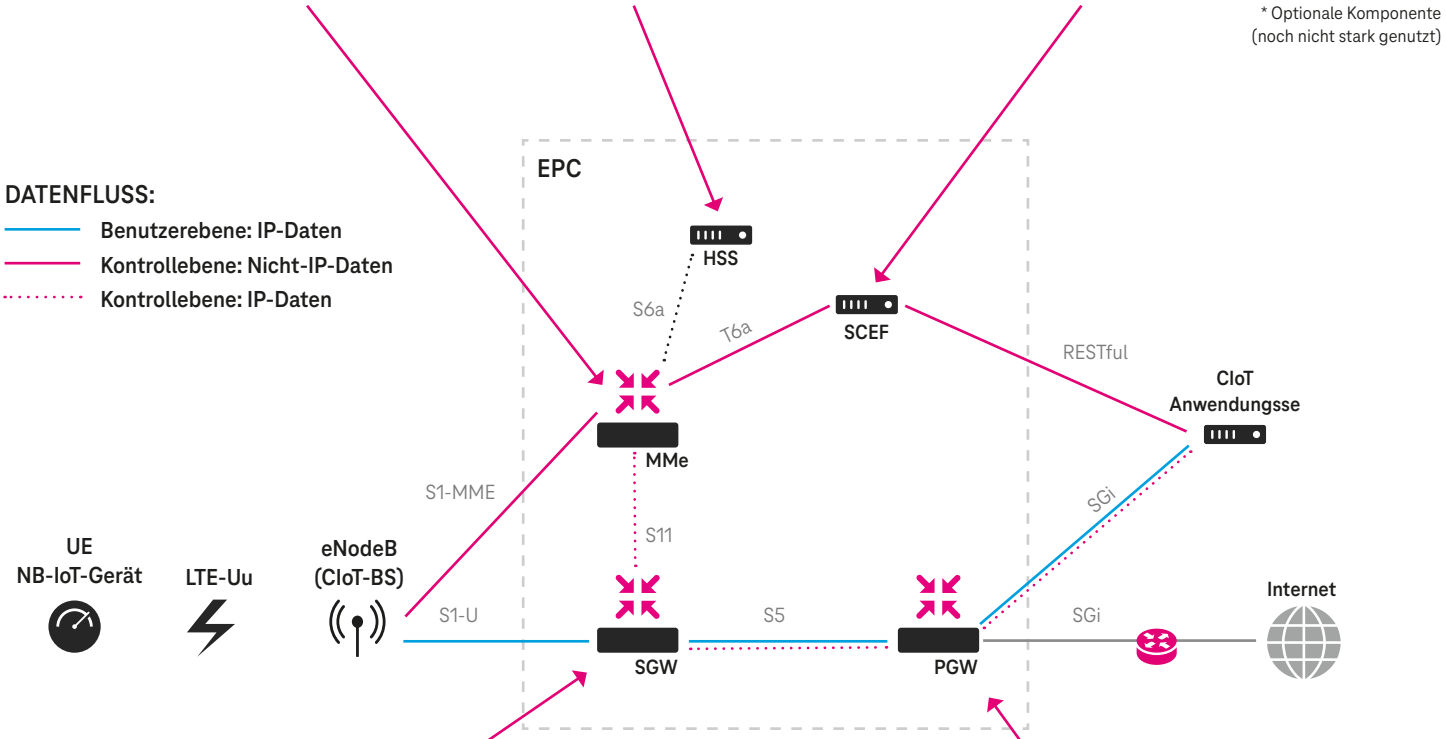
Home Subscriber Server (HSS)

⊕ Teilnehmerdatenbank
⊕ IMSI Hauptschlüssel K
⊕ Zulässige Dienste für UE

Service Capability Exposure Function (SCEF)*

⊕ Nicht-IP-Daten-Sendung

* Optionale Komponente (noch nicht stark genutzt)



Serving Gateway (SGW)

⊕ Datenpfadschaltung
⊕ Routing & Weiterleitung Benutzerdatenpakete

Packet Data Network Gateway (PGW)

⊕ Zuweisung: IP-Adresse

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

4.2.1. "Initial Attach"-Verfahren für NB-IoT-Geräte

Der Prozess der erstmaligen Verbindung eines Geräts mit einem NB-IoT-Netzwerk wird als anfängliches Anbindungsverfahren bezeichnet. Es umfasst zwei wichtige Schritte für die NB-IoT-Sicherheit. Gegenseitige Authentifizierung und Schlüsselvereinbarung (siehe Abbildung 9).

Authentifizierung

Um eine sichere Verbindung zwischen einem Endgerät und dem NB-IoT-Netzwerk herzustellen, müssen beide Parteien einander authentifizieren. Zu diesem Zweck enthält die USIM eine eindeutige Kennungsnummer, die die IMSI sowie einen Hauptschlüssel K mit 128 Bits Länge enthält. Der HSS speichert jede gültige SIM, ihren Hauptschlüssel K und ihre Autorisierungen. Für die gegenseitige Authentifizierung weisen das Endgerät und der HSS nach, dass sie im Besitz des Hauptschlüssels sind. Genau gesagt ist es jedoch die USIM – nicht das Gerät oder der Benutzer –, die sich gegenüber dem Netzwerk authentifiziert.

Das Endgerät sendet zuerst einen Anbindungsanfragebefehl mit ihrer IMSI an die MME. Die MME fordert daraufhin einen Authentifizierungsvektor (AV) vom HSS an. Der HSS generiert den Authentifizierungsvektor aus dem Hauptschlüssel K, einem Zähler (SQN) und einer zufälligen Nonce (RAND). Der endgültige Vektor enthält RAND, einen Token für die Netzwerkauthentifizierung (AUTN), eine erwartete Antwort während der Authentifizierung (XRES) sowie einen Schlüssel (KASME). Nach Eingang des Authentifizierungsvektors vom HSS, leitet die MME RAND und AUTN an das USIM des Benutzers weiter. Dieses berechnet eigenständig einen Authentifizierungsvektor. Es vergleicht das eigene AUTN-Token mit dem durch den MMS gesendeten Token. Wenn beide Werte übereinstimmen, wird das Netzwerk authentifiziert, da es bewiesen hat, dass es den zuvor gemeinsam verwendeten geheimen Schlüssel K kennt. Zudem generiert das Gerät seinen eigenen RES-Wert auf der Basis des gemeinsam verwendeten geheimen Schlüssels K und sendet ihn an die MME. Schließlich vergleicht die MME RES und XRES, um das Engerät zu authentifizieren. [24] Wenn die Benutzerauthentifizierung fehlschlägt, wird die Verbindung zum Nutzerendgerät beendet.

Schlüsselvereinbarung (key agreement)

Wenn die gegenseitige Authentifizierung erfolgreich ist, kann eine sichere Datenkommunikation hergestellt werden. Die zu verwendenden Integritäts- und Verschlüsselungsalgorithmen werden während der anfänglichen Anbindung vereinbart und basieren auf den Funktionen des Geräts und des Netzwerks. Während der Schlüsselvereinbarung werden unnötige Übertragungen von Schlüsseln vermieden. Stattdessen werden die Schlüssel von den betreffenden Parteien separat generiert, und zwar erst nach einem erfolgreichen Authentifizierungsverfahren.

Aus dem Schlüssel KASME werden zwei Schlüssel für Identitäts- und Vertraulichkeitsschutz abgeleitet: KNASenc und KNASint. Diese Schlüssel werden verwendet, um die NAS-Schicht der Kontrollbene sicher zu konfigurieren. Zudem generiert die MME den Schlüssel KeNB aus KASME und sendet ihn an den eNodeB. Das UE leitet denselben Schlüssel unabhängig ab. UE und eNodeB generieren daraufhin den Integritätsschlüssel KRRCint und den Verschlüsselungsschlüssel KRRCenc, die verwendet werden, um die AC-Schicht der Kontrollebene zu sichern. Die Kontrollebene kann somit zwischen dem Mobilgerät und der MME komplett gesichert werden. Um die Benutzerebene zu sichern, berechnen UE und eNodeB den Verschlüsselungsschlüssel KUPenc. Damit wird die Vertraulichkeit der Benutzerebene zwischen diesen beiden Komponenten sichergestellt. Zudem können MNOs entscheiden, einen IPsec-Tunnel von der Basisstation zum Kernnetzwerk zu implementieren. Dies ist beispielsweise für das Netz der Deutschen Telekom der Fall. Ein IPsec-Tunnel ist aufgrund des Vertraulichkeits- und Integritätsschutzes sowie der Authentifizierung der Kommunikationsendpunkte äußerst sicher. [9]

Sichere SIM-Karte schützt Schlüsselmaterial

Anders als viele LoRaWAN-Endgeräte sind NB-IoT-Geräte mit einer SIM-Karte ausgestattet, die ein sicheres Element darstellt, und daher manipulationsgeschützt sind. Somit lassen sich kryptografische Daten, wie etwa der Hauptschlüssel K, nicht ohne Weiteres aus der SIM extrahieren. [24] Zudem hat die Deutsche Telekom eine sichere SIM für preiswerte IoT-Geräte in Zusammenarbeit mit führenden Partnern der Branche entwickelt: Die nuSIM ist eine integrierte SIM, die niedrige Kosten und geringen Energieverbrauch gewährleistet und gleichzeitig die Sicherheit des LTE-Standards bietet [1]. SIM-Hersteller werden regelmäßig von der GSMA zertifiziert und arbeiten mit hochsicheren Rechenzentren zusammen.

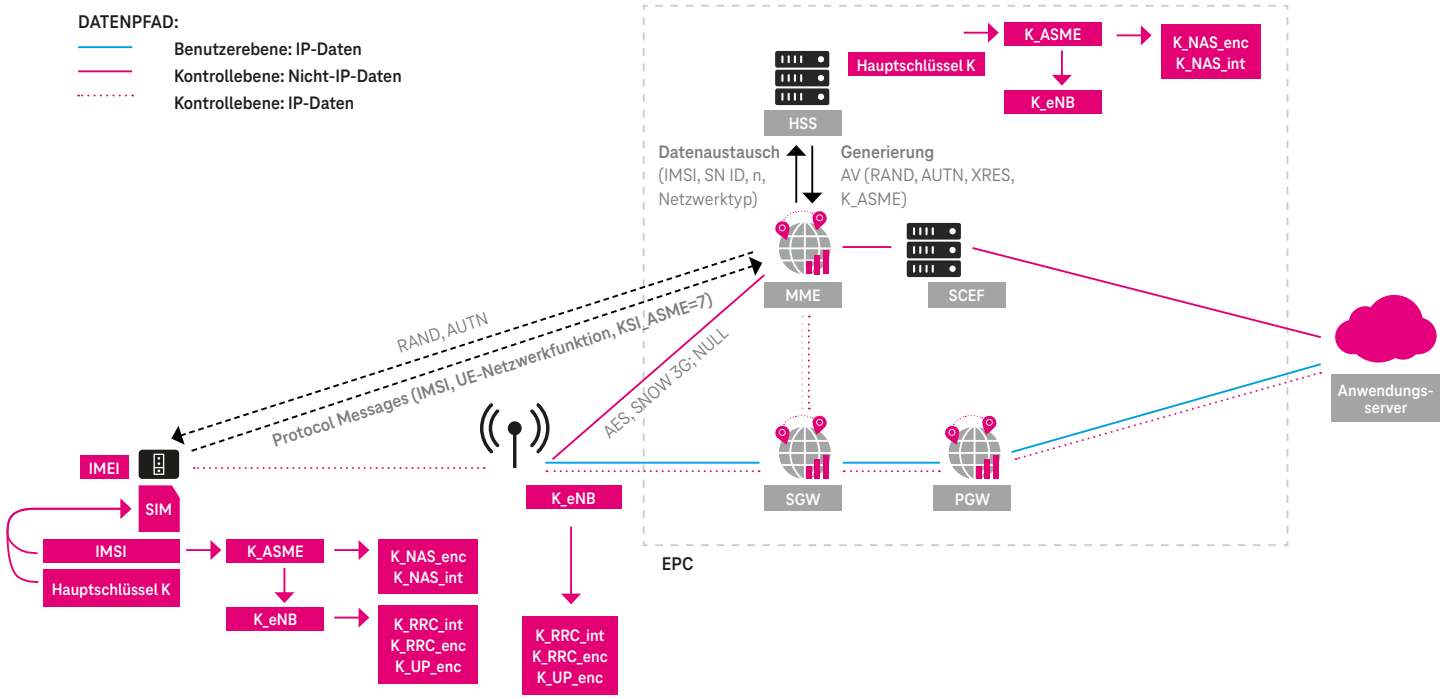


Abbildung 9: Anbindungsanfrage und Schlüsselvereinbarung/-austausch

Vorteile des anfänglichen Anbindungsverfahrens im NB-IoT

Vorteile:

- **Ausdrücklichegegenseitige Vereinbarung** auf der Basis des zuvor gemeinsam verwendeten geheimen Schlüssels in SIM und HSS
- **Sichere Schlüsselgenerierung**
- **SIM ist ein sicheres Element**

4.2.2. Daten-übertragung

Der Protokollstapel von NB-IoT, kategorisiert nach Kontroll- und Benutzerebene, ist in Abbildung 11 dargestellt. Schicht 1 und 2 der Protokolle PHY, MAC und PLC der Luftschnittstelle sind nicht geschützt. In NB-IoT-Netzwerken ist jedoch die Verbindung zwischen UE und eNodeB auf der PDCP-Schicht (Teil von Schicht 2) durch die Sicherheitskonfiguration der Zugriffsschicht (AS) gesichert. Auf der Benutzerebene werden IP-Pakete durch Verschlüsselung geschützt. Die 3GPP-Spezifikation definiert, dass Pakete der Benutzerebene an der Luftschnittstelle nicht integritätsgeschützt werden. Auf der Kontrollebene hingegen sichert die AS die Übertragung von RRC-Paketen durch einen Integritäts- und Verschlüsselungsalgorithmus.

Dank der Sicherheitskonfiguration der Nichtzugriffsschicht (NAS) weist die Kontrollebene ein zusätzliches Sicherheitsniveau der oberen Schicht auf. Während die Nichtzugriffsschicht am eNodeB endet, schützt das NAS-Protokoll die Integrität und Vertraulichkeit der Verbindung zwischen UE und MME. Wenngleich NAS und AS Verschlüsselung unterstützen, schreibt 3GPP keinen Vertraulichkeitsschutz vor. Stattdessen bleibt dieser dem Netzbetreiber als Option überlassen. [9] [24] Da die Kontrollebene von LTE-Netzen besser geschützt ist als die Benutzerebene, verwenden Kunden der Deutschen Telekom grundsätzlich die Kontrollebene für NB-IoT-Payload-Daten. Dies ist auch bei anderen Betreibern üblich. So werden sie nicht nur verschlüsselt, sondern auch gegen Manipulation geschützt – auf zwei Ebenen statt auf einer Ebene.

Für die Sicherung der Kommunikation zwischen Basisstation und Kernnetzwerk verwendet die Deutsche Telekom zudem Sicherheitstunnel. Zusätzlich kommen Netzwerkprotokolle und sichere Transportprotokolle (z. B. IPSec-Tunnel) zum Einsatz, um die Infrastruktur in den Räumlichkeiten des Kunden mit dem Kernnetzwerk zu verbinden.

Aufgrund der Standardisierung des 3GPP werden lediglich Sicherheitsmechanismen pro Abschnitt definiert. Ende-zu-Ende-Verschlüsselung wird nicht per se definiert und implementiert. Zudem ermöglichen NB-IoT-Netzwerke verschiedene Verschlüsselungs- und Integritätsverfahren (wie bereits in Kapitel 2 beschrieben). Die verfügbaren Verfahren sind in Tabelle 9 zusammen mit dem entsprechenden Verschlüsselungsalgorithmus aufgelistet. Das bedeutet: Der MNO kann das Niveau der Verschlüsselung selbst auswählen – während die EEA0- und EIA0-Verfahren (keine Verschlüsselung/Integrität) nur für Notrufe verwendet werden sollen. Die Deutsche Telekom nutzt beispielsweise EEA2- und EIA2-Verfahren aufgrund ihrer hohen Sicherheit.

Wenngleich die Spezifikation Ende-zu-Ende-Verschlüsselung nicht definiert, ist es möglich diese zu implementieren, indem man das Protokoll Datagram Transport Layer Security (DTLS) oder das leistungsfähigere BEST-Protokoll verwendet (siehe auch Kapitel 2). BEST wird jedoch noch nicht angeboten. Neben der 3GPP-Funktion für die Ende-zu-Ende-Verschlüsselung werden weitere Lösungen von Organisationen mit offenen Standards sowie von Hardware- und Cloud-Anbietern eingeführt.

Chiffrebezeichner	Methode	Integritätsbezeichner	Methode
EEA0	NULL (keine Verschlüsselung)	EIA0	NULL (keine Integrität)
EEA1	SNOW 3G	EIA1	SNOW 3G
EEA2	AES-CTR	EIA2	AES CMAC

Tabelle 9: Verschlüsselungs- und Integritätsverfahren in NB-IoT-Netzwerken [9]

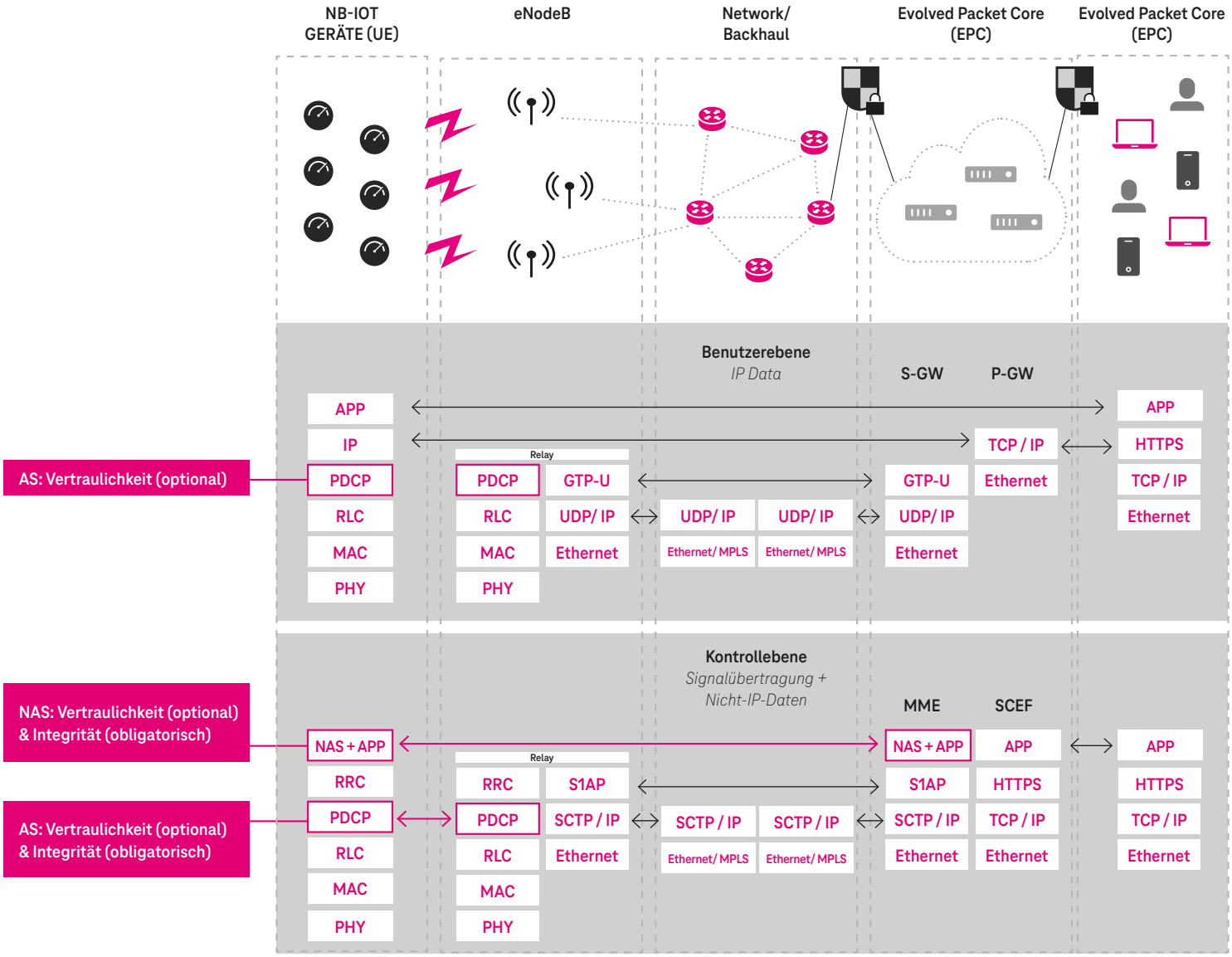


Abbildung 10: Protokollstapel und Sicherheitsmechanismus LTE/NB-IoT [26]

Vorteile:

- ⊕ **Verschlüsselung** verfügbar für Benutzer- und Kontrollebene an der Luftschnittstelle sowie für die Kontrollebene zwischen UE und MME
- ⊕ **Data over NAS** ermöglicht, dass Benutzerdaten sicherer über die Kontrollebene gesendet werden

Nachteile:

- ⊖ **Die Auswahl von einem der vier Verschlüsselungsalgorithmen** bleibt dem Netzbetreiber überlassen
- ⊖ **Kein Integritätsschutz** für die Benutzerebene
- ⊖ **Keine Ende-zu-Ende-Verschlüsselung**

Tabelle 10: Vorteile und Nachteile der NB-IoT-Datenübertragung

4.2.3 Schwachstellen von NB-IoT

Das Risiko erfolgreicher Cyberangriffe auf LTE kann jedoch lediglich gemindert werden. Wie bereits oben erwähnt, überlässt 3GPP die Verschlüsselung als Option den MNOs und untersagt sogar den Integritätsschutz des Verkehrs auf Benutzerebene. Laut dem US-amerikanischen NIST-Institut sind RF-Störangriffe gegen LTE-Netze machbar. Zudem werden NB-IoT und LTE zumeist zusammen mit weniger sicheren UMTS-(3G-) oder GSM-(2G-)Netzen implementiert.

So soll ein Endgerät in der Lage sein, sich mit einem 3G- oder 2G-Netz zu verbinden, wenn kein LTE-Zugang verfügbar ist. Dies erhöht jedoch die Angriffsfläche. Für Anrufsignalisierung in GSM und UMTS wird ein separates Netzwerk verwendet, das auch Roaming ermöglicht: das SS7-Netz. SS7 zeigte in der Vergangenheit verschiedene Sicherheitsprobleme. Einige dieser Probleme wurden beim LTE-Roaming behoben, andere sind jedoch nach wie vor ungelöst.

NB-IoT-Netzwerke greifen umfassend auf die IP-Technologie zurück. IP ist bei Sicherheitsexperten wie auch bei Cyberkriminellen weithin bekannt. Dies kann gleichermaßen ein Vorteil und ein Nachteil sein. Einerseits existieren bewährte IP-Sicherheitstechnologien, die implementiert werden können, um NB-IoT zu sichern. Andererseits kennen Angreifer die Schwächen von IP-Netzwerken und halten entsprechende Tools bereit. [24]

5. Fazit

Zusammenfassend lässt sich sagen, dass NB-IoT und LoRaWAN starke Sicherheitsmechanismen aufweisen (siehe auch Tabelle 11). NB-IoT ist ein offener Standard des 3GPP und basiert auf LTE. Damit profitiert er stark von seinen Sicherheitsmechanismen auf der Basis des LTE-Funkstandards: Das Sicherheitskonzept wurde sehr detailliert entwickelt und gründlich getestet. LoRaWAN ist ein von der LoRa Alliance entwickeltes Protokoll und basiert auf einer proprietären Modulation. Dennoch weist es wichtige Sicherheitsfunktionen auf. Während NB-IoT ein lizenziertes Spektrum nutzt, greift LoRa-WAN auf ein unlizenziertes Spektrum zurück. LoRaWAN ist somit anfälliger für RF-Störung, wenngleich eine sehr robuste Modulation zum Einsatz kommt.

Der Prozess der Integration eines Endgeräts in ein NB-IoT-Netzwerk wird durch das LTE-Verfahren der anfänglichen Anbindung gut gesichert, einschließlich gegenseitiger Authentifizierung und sicherer Schlüsselgenerierung. Zudem werden die Schlüssel äußerst sicher verteilt, dank manipulationssicherer USIMs und SIM-Anbieter, die regelmäßig von der GSMA zertifiziert werden und hochsichere Rechenzentren in Anspruch nehmen. LoRaWAN bietet zwei Optionen für dieses Verbindungsverfahren. Eine Option, ABP, ist unsicher und wird nicht empfohlen. Die zweite Option, OTAA, weist hingegen wichtige Sicherheitsfunktionen auf, ist aber in der am meisten genutzten Version v1.0 fehleranfällig. Dies betrifft insbesondere den Schlüsselgenerierungsprozess.

Als Verschlüsselung bietet LoRaWAN Ende-zu-Ende-Verschlüsselung. Der einzige Nachteil liegt darin, dass der Netzwerk-Vermittlungsserver den Verschlüsselungsschlüssel für Anwendungsdaten in v1.0 generiert. Der NB-IoT-Standard beinhaltet lediglich eine optionale Verschlüsselung für die Benutzerebene und die Kontrollebene an der Luftschnittstelle sowie für die Kontrollebene zusätzlich zwischen Endgerät und MME. Diese Verschlüsselungsoptionen sind jedoch in den NB-IoT-Netzwerken der Deutschen Telekom obligatorisch. Ende-zu-Ende-Verschlüsselung kann mithilfe von DTLS oder dem künftigen leistungsfähigen BEST-Standard implementiert werden. Darüber hinaus ist die Ende-zu-Ende-Verschlüsselung auf der Anwendungsschicht über das OSCORE-Protokoll möglich, das besonders gut für IoT-Frameworks geeignet ist, die CoAP verwenden, wie OMA Specworks Lightweight M2M (LwM2M) und Open Connectivity Foundation/IoTivity (OCF) [27]. Dies wird vor allem für Roaming-Anwendungen und sicherheitssensible Anwendungen empfohlen, da Anbieter wie die Deutsche Telekom bereits zusätzliche Sicherheitsmechanismen (z. B. IPsec-Tunnel) zwischen dem Kernnetzwerk und den Anwendungsservern einsetzen. LoRaWAN nutzt das sichere Verschlüsselungsverfahren AES-128. Für NB-IoT können Anbieter zwischen verschiedenen Algorithmen wählen. Die Deutsche Telekom verwendet beispielsweise ebenfalls AES.

Integrität wird für komplette LoRaWAN-Frames zwischen Endgerät und Netzwerkserver gewährleistet und somit nicht Ende-zu-Ende. In NB-IoT-Netzwerken ist der Integritätsschutz auf die Kontrollebene beschränkt und wird zwischen Endgerät und Basisstation sowie zwischen Endgerät und MME eingesetzt. Die Deutsche Telekom überträgt jedoch NB-IoT-Daten über die Kontrollebene – dank der Data-over-NAS-Technologie – und wendet Integrität somit auch für Benutzerdaten an.

Für NB-IoT-Anwendungsfälle kann angenommen werden, dass der MNO in seinem Heimnetzwerk über ein gut abgerundetes Sicherheitskonzept verfügt. Die konstante Arbeit des 3GPP sowie der Sicherheitsforscher in aller Welt bewirkt, dass LTE-Sicherheit – und damit NB-IoT-Sicherheit – ständig verbessert wird. Die Sicherheit von LoRaWAN-Netzwerken hängt hingegen stark von der umfassenden Nutzung der LoRaWAN-Architektur v1.1 ab , die bis heute nicht allgemein bereitgestellt wird.

Unabhängig von der Technologie werden die sichere Implementierung von Funktionen sowie der korrekte und sichere Aufbau von Systemen zunehmend relevant. Daher sollten Organisationen grundsätzlich das Sicherheitskonzept in Frage stellen und individuelle Risikobewertungen und Risikominderungsmaßnahmen durchführen.

Insgesamt liegt der entscheidende Vorteil von NB-IoT gegenüber Lo-RaWAN in der sicheren Speicherung der kryptografischen Schlüssel. Das bedeutet: Während NB-IoT-Schlüssel voraussichtlich nicht aus der SIM oder den Rechenzentren der Hersteller extrahiert werden, sind viele LoRaWAN-Geräte nicht manipulationssicher, und es be- steht die Möglichkeit, dass geheime Schlüssel an Black-Hat-Hacker preisgegeben werden.

	LoRaWAN	NB-IoT
Standardisierung	• LoRaWAN (MAC-Schicht): Spezifikation entwickelt und gepflegt von der LoRa Alliance • LoRa (physische Schicht): proprietär, patentiert von Semtech	• Offener Standard von 3GPP • Basiert auf LTE
Spektrum	• Unlizenziertes Spektrum • Modulation basiert auf sehr robustem und schwer zu empfangendem Chirp Spread Spectrum (CSS)	• Lizenziertes Spektrum • Modulation basiert auf den robusten OFDMA/ SC-FDMA-Verfahren
Verbindungsmethoden	• ABP: schnell, aber sicher aufgrund von perma-nenten Schlüsseln • OTAA: sichere Methode, abgesehen von geringfügigen Beschränkungen, verbessert mit LoRaWAN v1.1	• Erstangriff: sichere Anbindung aufgrund gegenseitiger Authentifizierung sowie sichere Schlüsselgenerierung und sicherer Schlüsselaustausch
Verschlüsselung	• Ende-zu-Ende-Verschlüsselung für Frame-Payloads standardmäßig	• Verschlüsselung zwischen Endgerät und eNodeB auf Schicht 2 der Benutzer- und Kontrollebene • Verschlüsselung zwischen Endgerät und MME auf NAS-Schicht der Kontrollebene • Standardmäßig keine Ende-zu-Ende-Verschlüsselung, kann aber beispielsweise durch DTLS, BEST, oder OSCORE realisiert werden
Verschlüsselungsalgorithmus	• AES-128 im CCM-Modus	• Der MNO kann einen Stromchiffre-Verschlüsselungsalgorithmus auswählen, z. B. auf der Basis von SNOW 3G, AES-128-CTR • AES-CTR ist Standard in den Netzen der Deutschen Telekom
Integrität	• Integritätsschutz des Headers und der Payload von MAC-Frames zwischen Endgerät und Netzwerkserver • Keine Integrität zwischen Netzwerk und Anwendungsserver	• Integritätsschutz zwischen Endgerät und eNodeB auf Schicht 2 und zwischen Endgerät und MME auf NAS-Schicht der Kontrollebene • Kein Integritätsschutz der Benutzerebene, aber Funktion, die den Transport von Benutzerdaten über die sicherere Kontrollebene ermöglicht
Integritätsalgorithmus	• AES-128-CMAC	• Der MNO kann einen Verschlüsselungsalgorithmus auswählen, z. B. SNOW 3G, AES-128-CMAC
Endgerätesicherheit	• **Zumeist keine sichere Schlüsselspeicherung** aufgrund eines fehlenden sicheren Elements im LoRaWAN-Endgerät	• **Sicheres Element** in der SIM-Karte schützt Schlüssel vor Extraktion • **Zertifizierte hochsichere Rechenzentren** werden von SIM-Herstellern genutzt
Schwachstellen	• **RF-Störangriffe** sind einfacher als im lizenzierten Spektrum • **Physische Angriffe** sind kritisch, aber problemlos erkennbar • **Architektur v.1.0** weist verschiedene bekannte Sicherheitsschwachstellen auf (z. B. beschränkte Ende-zu-Ende-Verschlüsselung durch vorübergehenden Besitz des Schlüssels durch den Netzwerk-Vermittlungsserver), ist aber nach wie vor die Architektur mit der größten Verbreitung. • **Architektur v.1.1** wurde verbessert, aber ein Austausch der Firmware ist weiterhin möglich, wie auch Self-Replay-Angriffe und bösartige Endpunktangriffe	• **In Roaming-Protokollen** wurden in der Vergangenheit Sicherheitsschwachstellen erkannt • **Die Erzwingung der Nutzung von GSM durch die Geräte** stellt ein Risiko dar • **RF-Störangriffe** sind machbar • **Bösartige Basisstationen** lassen sich problemlos aufbauen, sind aber schwer in ein gültiges Netzwerk zu integrieren

Tabelle 11: Zusammenfassung der Sicherheitsfunktionen in NB-IoT und LoRaWAN

III. Quellen

[1] ..... Deutsche Telekom, Mobile IoT guide – how NB-IoT and LTE-M are helping the IoT take off. Bonn, 2019. [Online] Verfügbar: 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] Verfügbar: 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. Abgerufen unter 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] ..... 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, Bd. 40., Providence, Rhode Island: American Mathematical Society, 2019.

[8] ..... Teil 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, Bd. 7, Ausgabe 4, Nr. 4, Juli 2010, S. 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). Abgerufen unter https://www.design-reuse.com/news/28706/semtech-cycleo-acquisition.html

[14] ..... Schmidiger GmbH. (n.d.). Wie gut ist die Funktechnologie LoRa wirklich?. Abgerufen unter 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] Verfügbar: https://www.elektronik-kompendium.de/sites/kom/1509011.htm

[22] ..... 3GPP, LTE. [Online] Verfügbar: 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, S. 1–5.

[24] ..... J. Cichonski et al., Guide to LTE security. NIST Special Publication 800–187, 2017. [Online] Verfügbar: 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] Verfügbar: 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] Verfügbar: https://www.ericsson.com/en/blog/2019/11/oscore-iot-security-protocol

Hinweis: Auf alle oben genannten Web-Ressourcen wurden zwischen August und September 2020 zugegriffen.

Kontakt
iot@telekom.de
iot.telekom.com

Herausgeber
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn, Deutschland

Version 1.0, Januar 2021