Bild: Albert Hulm

Langstreckenfunk

IoT-Funk LoRaWAN: für kleine Datenmengen und hohe Reichweiten

Mit LoRaWAN bindet man zum Beispiel Sensoren und Location-Tracker ans Internet an. Das funktioniert auch ohne kommerziellen Netzanbieter. Die Initiative The Things Network verfolgt einen Community-Ansatz zum flächendeckenden Ausbau von LoRaWAN.

Von Jan Mahn

Als das große Zukunftsprojekt für den Mobilfunk wird immer wieder 5G gehandelt: Höhere Datenrate und niedrigere Latenz als bei LTE sind die Ziele, damit vor allem industrielle Nutzer noch mehr Daten senden und empfangen können [1]. Während der Ausbau von 5G noch nicht begonnen hat, entstehen bereits heute Funknetze, die sich in die entgegengesetzte Richtung entwickeln: Niedrigere Datenrate, weniger übertragene Daten. „Low Power Wide Area Networks“ (LPWAN) heißen diese Netzwerke. Gedacht sind sie für Geräte, die mit Sensoren ausgestattet sind und möglichst lange im Akkubetrieb aushalten müssen. Ein verbreitetes Protokoll für ein solches Funknetz heißt LoRaWAN. Die Besonderheit: LoRaWAN arbeitet im zuteilungsfreien Frequenzbereich bei 868 MHz. Das bedeutet, jeder kann ein LoRaWAN-Netz selbst aufbauen – oder eine Community-basierte Lösung nutzen.

Datensparsam

In der Werbesprache nennt man die Einsatzbereiche für solche Netze „Smart City“, „Smart Farming“ oder „Smart Transport“. Gemeint sind Szenarien, in denen Sensoren Messwerte aufnehmen, sie über Funk versenden, damit eine Software irgendetwas Nützliches damit anstellt. Parksensoren, in allen Parkflächen einer Stadt eingelassen, wären ein Beispiel – sie melden regelmäßig an einen Server, ob sie ein Auto erkannt haben. Für die Autofahrer werden dann Routen berechnet, die sie direkt zu einem freien Parkplatz führen.

Die Anforderungen an die Funkverbindung sind völlig anders als bei LTE oder 5G. Der Parksensor braucht zunächst keine ständige Verbindung zu einer Gegenstelle. Er wird die meiste Zeit des Tages im Tiefschlaf verbringen, also alle Komponenten abschalten und vielleicht alle fünf oder zehn Minuten aufwachen und messen. Nach der Messung verschickt er eine Nachricht – die Nutzlast der Nach-

richt muss nur 1 Bit lang sein, `true` oder `false`, frei oder besetzt. Selbst kompliziertere Sensoren, die zum Beispiel Temperatur, Luftfeuchte und Luftdruck messen, kommen nur auf wenige Byte Daten pro Messung. Nach dem Verschicken schaltet der eingebaute Prozessor das Funkmodul ab und wartet wieder fünf Minuten im Tiefschlaf. Während dieser Zeit muss er aus der Ferne nicht erreichbar sein.

Wünschenswert wäre es, wenn sich der Sensor beim Verschicken einer Nachricht mit seinem Namen melden würde, damit das Netzwerk die Nachricht richtig zuordnen und der Server die empfangenen Daten sinnvoll auswerten kann. Gleichzeitig sollte die Übertragung auch sicher sein. Wer Daten per Funk verschickt, darf sich nicht darauf verlassen, dass es schon niemand mitbekommen wird. Man muss immer davon ausgehen, dass jeder in Reichweite mit günstiger Hardware den Verkehr mitschneiden und auch eigene Nachrichten verschicken kann. Die wichtigsten Angriffszenarien, die dadurch entstehen, finden Sie im Kasten auf Seite 142.

LoRaWAN hält für alle skizzierten Anforderungen eine Lösung bereit. Die vollständige Spezifikation wird von der LoRa Alliance betreut und kann von deren Webseite heruntergeladen werden (zu finden über ct.de/y5ey). Hinter der Organisation stehen Chip- und Netzwerkkomponentenhersteller wie Semtech, ST Microelectronics und Cisco.

LoRa, LoRa

Die funktechnische Grundlage von LoRaWAN, also die Übertragungsschicht, heißt LoRa. Diese Technik wurde von Semtech entwickelt und ist proprietär. Semtechs Chips sind also in allen LoRa-Sendern und -Empfängern zu finden.

Die Eckdaten von LoRa sind aber bekannt: Gefunkt wird in zuteilungsfreien Frequenzbereichen, in Europa um 868 MHz (863–870 MHz). Das Übertragungsverfahren heißt „Chirp Spread Spectrum“ – ein sogenanntes Symbol, also die kleinste übertragene Einheit, ist eine Art Zirpen, also eine Sinuswelle mit gleichbleibender Amplitude, deren Frequenz sich verändert. Bei einem „Upchirp“ beginnt die Welle mit niedriger Frequenz, die erhöht wird. Ein „Downchirp“ beginnt mit höherer Frequenz, die während des Zirpens niedriger wird. Übersetzt auf den hörbaren Frequenzbereich würde das wie ein kurzer Pfeifton klingen, der höher oder tiefer wird. Diese Übertragungsart ist sehr unempfindlich gegenüber Störungen, die in einem zuteilungsfreien Frequenzbereich nicht selten sind. Die Zirp-Impulse erstrecken sich nämlich über eine große Bandbreite und sind so charakteristisch, dass der Empfänger sie mit sehr hoher Wahrscheinlichkeit wahrnimmt und es ihm vergleichsweise leicht fällt, die Signale vom Rauschen zu unterscheiden. Die Frequenz wird während eines Chirps um 125 kHz oder 250 kHz verändert. Die relativ hohe Bandbreite wird also nicht für hohe Datenraten ausgereizt, sondern für klar erkennbare Symbole genutzt.

Der LoRa-Nutzer kann einige Parameter für die Übertragung anpassen. Neben der Bandbreite des Chirps kann er auch auch dessen Dauer wählen, die als „Spread Factor“ bezeichnet wird. Je kleiner sie ist, desto mehr Daten können pro Zeiteinheit übertragen werden. Die Wahrscheinlichkeit, dass ein Chirp vom Empfänger wegen einer Störung nicht als solcher erkannt wird, steigt dadurch aber. LoRa arbeitet mit sechs verschiedenen Spread Factors, die als SF7 bis SF12 bezeichnet werden. Ein Chirp mit SF7 ist halb so lang wie ein Chirp mit SF8 und so weiter.

Die Wahl von Spread Factor und Bandbreite bestimmt, wie hoch die Datenrate sein kann und wie hoch die Empfangswahrscheinlichkeit: Wer sicher gehen will, dass die Nachricht ankommt, sendet mit der langsamsten Kombination, die in der Spezifikation vorgesehen ist: SF12 bei 125 kHz kommt auf 250 Bit/s. Die schnellste spezifizierte Kombination ist SF7 bei 250 kHz Bandbreite. Damit kommt man auf immerhin 11000 Bit/s. Für welche Kombination sich der Entwickler eines LoRa-Senders entscheidet, hängt von seinem Anforderungsprofil ab. Für schnelle Übertragungen spricht, dass sie schneller erledigt sind. Prozessor und Sender müssen kürzer laufen und die Batterie belasten, bevor sie wieder in den Tiefschlaf verfallen dürfen.

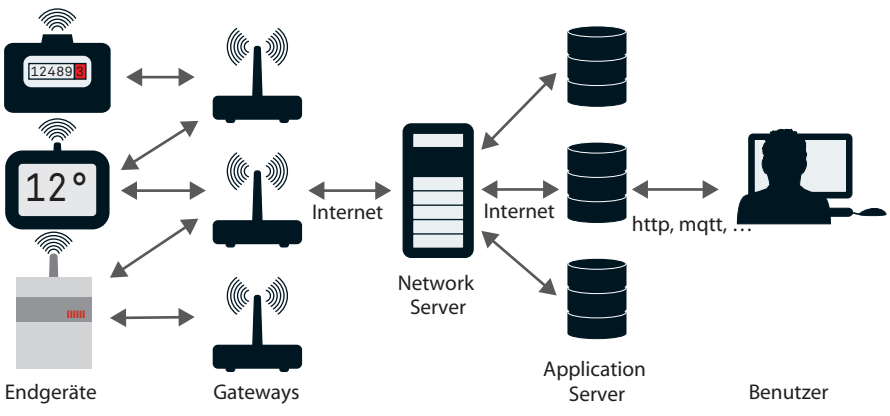
Wie groß der Abstand zwischen LoRa-Sender und Empfänger sein darf, kann man nicht pauschal beantworten – neben Spreading Factor und Bandbreite sind auch die Sendeleistung des LoRa-Chips und die verwendete Antenne entscheidend. In der Stadt kann man schon mit einer kleinen Drahtantenne mit 1/4 der Wellenlänge (8,63 cm) mit über 500 Metern rechnen. Mit niedriger Datenrate sind auch mehrere Kilometer möglich, auf dem Land weit darüber hinaus.

Paketzusteller

Mit LoRa allein kann man zwar Daten zuverlässig in die Welt verschicken. Um diese zu empfangen und zu verarbeiten, braucht es aber ein Netz aus Empfangsstationen – das ist Aufgabe von LoRaWAN. Die Empfänger sind sogenannte Gateways, die auf der einen Seite den Funk bei 868 MHz auf LoRa-Chirps abhören und auf der anderen Seite über das Internet mit den sogenannten Network Servern des LoRaWAN verbunden sind. Diese Server sind dafür zuständig, den Absender zu identifizieren und das Paket an einen Application Server weiterzuleiten, bei dem der Besitzer des Sensors es abrufen kann.

Nachrichten-Verarbeitung im LoRaWAN

Die Gateways leiten alle Nachrichten an den Network Server weiter. Der prüft die Signatur und übergibt die Nachricht an den zuständigen Application Server.



Eine Nachricht kann von einem oder mehreren Gateways empfangen werden. Diese Gateways leiten sie ohne weitere Eingriffe an die Network Server weiter. Damit diese wissen, von welchem Endgerät die Nachricht verschickt wurde, muss sie mehr enthalten als die reinen Nutzdaten. Jedes Gerät bekommt vom Betreiber des Network Servers eine Geräte-ID (DevAddr) mit einer Länge von 32 Bit. Außerdem einen Schlüssel mit einer Länge von 128 Bit: Mit dem Network Session Key (NwkSKey) generiert es eine 32 Bit lange Signatur, den Message Integrity Code (MIC) aus seiner Adresse, einem Counter und der Nachricht. Die Network Server kennen den Schlüssel und können anhand der Signatur sicherstellen, dass die Nachricht von einem bekannten Gerät stammt. Außerdem wissen sie, welcher Application Server für das Gerät zuständig ist. Dieser bekommt die Nachricht jetzt zugestellt.

Auch der Application Server hat einen Schlüssel an das Endgerät ausgegeben: Mit dem Application Session Key (AppSKey) verschlüsselt es die eigentliche Nachricht, als Verfahren kommt AES zum Einsatz. Nur dieser Server ist in der Lage, den Inhalt zu entschlüsseln. Der Besitzer des Geräts kann die Nachricht sich beim Server über eine Weboberfläche, ein HTTP-API oder MQTT abholen. Das Netzwerk kümmert sich auch darum, dass eine Nachricht nur einmal beim Nutzer ankommt, auch wenn viele Antennen sie abgefischt haben.

LoRaWAN kennt auch einen Rückweg, also eine Datenübertragung zum Endgerät. Diese ist bei tiefschlafenden Sensoren (die Spezifikation nennt sie „Class A“) aber nicht jederzeit möglich. Stattdessen kann ein Gerät nach einer Übertragung von Messwerten kurz auf Antworten warten, die das Netzwerk bereithält. So könnte man dem Sensor zum Beispiel nach einer Messung eine neue Schlafzeit übergeben.

Alle zusammen

Die Gateways eines LoRaWAN können über die ganze Welt verteilt sein. Sie müssen nur über das Internet oder ein lokales Netz mit einem Network Server verbunden sein (die wiederum mit einem Application Server). Ein Industrieunternehmen könnte beispielsweise zehn LoRaWAN-Gateways aufstellen und einen eigenen Server betreiben. Eine Open-Source-Implementierung für LoRaWAN ist die Software LoRaServer, zu finden über ct.de/y5ey. Sie vereint beide Server-Rollen auf einer Maschine.

Bei LoRaWAN ist es nicht einmal wichtig, dass man den Betreibern der Gateways vertrauen kann. Selbst wenn diese sämtlichen Verkehr mitschneiden, können sie mit den Nachrichten keinen Schaden anrichten. Vertrauen muss man nur dem Network Server, dass er zustellt, und dem Application Server, der die Inhalte entschlüsseln kann.

Da LoRa im zuteilungsfreien Frequenzbereich arbeitet und potenziell jeder ein Gateway betreiben kann, der einen Internetanschluss besitzt, kam eine Initiative aus den Niederlanden im Jahr 2015 auf die Idee, ein weltweites Community-LoRaWAN aufzubauen: The Things Network (TTN) war geboren. Die Organisation betreibt Network Server und Application Server, Freiwillige stellen die Gateways zu Hause oder an exponierten Standorten auf. Wer ein eigenes LoRaWAN-Projekt plant und ein TTN-Gateway betreibt, versorgt immer auch seine Umgebung. Das macht LoRaWAN interessant für Bastler und kommerzielle Nutzer gleichermaßen. In den Niederlanden haben sie schnell ein fast flächendeckendes Netz aufgebaut. In Deutschland gibt es bisher nur einige größere Städte mit lückenloser Abdeckung. Die Karte auf thethingsnetwork.org/map zeigt die Standorte aller Gateways. Neben privaten Bastlern sind es vor allem Universitäten, die Gateways im Einsatz haben. Unter den Betreibern sind aber auch Überraschungen: Am Berliner Hauptbahnhof betreibt zum Beispiel die Deutsche Bahn mehrere Gateways – eine Anwendung ist die Überwachung von Bahnhofsuhren, wie ein Bahn-Mitarbeiter im Rahmen einer Bitkom-Konferenz erläuterte (Video und Folien siehe ct.de/y5ey).

Bis Anfang des Jahres 2019 war die Anschaffung eines Gateways für Privatleute wenig attraktiv. Das „The Things Gateway“, das von TTN entwickelt wurde, kostete knapp 300 Euro. Auf der eigenen Konferenz stellten die Initiatoren im Januar aber zwei neue Gateways vor: Das „The Things Indoor Gateway“ ist ein kleines Steckdosengerät, das sich mit einem WLAN verbindet und eine eingebaute Antenne für LoRa hat. Für 85 Euro kann man es aktuell vorbestellen, Mitte Juni soll es verfügbar sein.

Angriffe auf Funkübertragungen

Werden Daten per Funk verschickt, kann jeder in Reichweite mit einem passenden Empfänger die Nachrichten mitschneiden und auslesen. Zwei Probleme können dadurch entstehen: Der Angreifer kann sensible **Informationen mitlesen**. Bei einem Temperatursensor mag das verschmerzbar sein, versendet man dagegen Statusinformationen einer Industrieanlage, sollte die verschickte Nachricht, die Nutzlast, verschlüsselt sein.

Das zweite Problem ist die **Integrität** der Daten. Wer eine Nachricht mitgelesen hat, kann schnell eigene Meldungen abschicken. Unternimmt man nichts weiter, kann der Empfänger nicht überprüfen, ob der Absender wirklich der Sensor oder ein Angreifer war. Als Schutzmaßnahme sendet man eine Signatur mit – dazu generiert man mit einem geheimen Schlüssel aus der übertragenen Nachricht und dem Namen des Absenders einen Hashwert. So kann der Empfänger, der den passenden Schlüssel kennt, prüfen, ob diese Nachricht unverfälscht ist.

Wer eine gültige Nachricht mit Signatur mitgeschnitten hat, könnte diese aber immer noch speichern und später noch einmal absenden – die Signatur ist ja gültig und der Empfänger akzeptiert sie. Dieser Angriff wird als **Replay-Attacke** bezeichnet. Hat man beispielsweise einen Sensor, der einen Alarm meldet, könnte man mühelos falschen Alarm auslösen, wenn man eine Alarmnachricht kennt. Als Schutz fügt man an die Nachricht eine Zahl an, die mit jedem Paket erhöht wird. Dieser Counter wird ebenfalls bei der Berechnung der Signatur benutzt. Der Empfänger wird angewiesen, nur noch Nachrichten zu berücksichtigen, bei denen der Counter höher ist als der der letzten Nachricht. Eine mitgeschnittene Nachricht wird für den Angreifer wertlos.

Neben diesen fertigen Lösungen findet man auf der Seite des Netzwerks auch Bauanleitungen für eigene Gateways auf Basis eines Raspberry Pis. Benötigt wird aber ein sogenanntes Concentrator-Board, das mit etwa 150 Euro zu Buche schlägt. Mit der Verfügbarkeit der Indoor Gateways werden diese Lösungen uninteressanter.

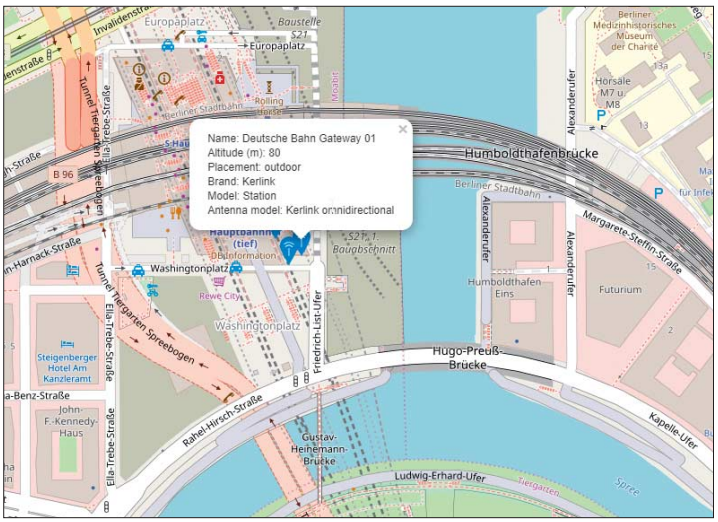
Startpunkt

Wer schon eine TTN-Abdeckung zu Hause hat und ein eigenes Sensor-Bastel-Projekt plant, muss sich für eine Entwicklungs-Plattform entscheiden. In der Arduino-Welt gibt es den „Arduino MKR WAN 1300“, einen Arduino Zero mit LoRa-Modul. Wer seine Projekte lieber mit dem ESP32 angeht, findet auf einschlägigen Handelsplattformen unter dem Suchbegriff „esp32 lora“ passende Boards mit USB-Anschluss, optional auch mit einem kleinen OLED-Display.

Will man mit einem beliebigen Mikrocontroller eine eigene Schaltung aufbauen, die Nachrichten per LoRa an The Things Network verschickt, ist der RFM95 von Hope RF ein geeigneter Kandidat – die kleine Platine ist für weniger als zehn Euro zu haben. Beim Kauf sollte man als Europäer darauf achten, die Version mit 868-MHz-Modul zu suchen. In einer der nächsten Ausgaben von c’t geht es um den Eigenbau eines besonders stromsparenden LoRa-Sensors, in dem dieser Chip zum Einsatz kommt.

Um die grundlegende Funktionsweise der Weboberfläche und Begrifflichkeiten von TTN kennenzulernen, braucht man aber noch keine Hardware. Zu Beginn muss man einen kostenlosen Account anlegen. Auf der Webseite findet man dafür oben rechts den Button „Sign Up“. Nach der Registrierung und Bestätigung der Mailadresse findet man die Oberfläche unter console.thethingsnetwork.org. Zwei Dinge kann man hier anlegen: „Gateways“ und „Applications“ – die Grenzen zwischen Application Server und Network Server verschwimmen hier, da TTN beide Dienste übernimmt. Eine Application ist eine Sammlung von Geräten, die thematisch zusammengehören. Mit „add application“ erzeugen Sie eine solche. Angeben müssen Sie einen Namen, der im gesamten Netzwerk einmalig sein muss. Eine Beschreibung ist optional.

Im Abschnitt „Devices“ können Sie Hardware hinzufügen. Abgefragt wird eine „Device ID“, also ein Name, der innerhalb der Application einmalig ist, zum Beispiel



Auch die Deutsche Bahn beteiligt sich an The Things Network und betreibt öffentliche LoRaWAN-Gateways in Berlin

„temperatur-garten“. Die anderen Werte füllt TTN selbst aus. Auf der Übersichtsseite sehen Sie jetzt alle Werte zum Gerät, die Sie benötigen, um sie in den eigenen Code einzufügen. LoRaWAN kennt zwei Verfahren, mit denen die beiden benötigten Schlüssel (AppSKey und NwkSKey) auf dem Gerät landen. TTN unterstützt sie beide: Bei der Over-the-Air-Activation (OTAA) muss der Entwickler auf dem Gerät die ID der Anwendung (Application EUI) und den Anwendungsschlüssel (App Key) hinterlegen. Mit diesen Angaben und der „DevEUI“, einer 64-Bit-Zeichenfolge, die vom Chiphersteller eingebaut wurde, kann es sich beim ersten Start beim Netzwerk melden. Als Antwort bekommt es die Schlüssel und die DevAddr.

Für die ersten Versuche mit einer Entwicklungsumgebung Ihrer Wahl empfiehlt es sich, das Verfahren auf „Activation by Personalization“ (ABP) umzustellen. Dabei bekommt das Gerät Schlüssel und Adresse hartkodiert. Klicken Sie dazu oben rechts auf „Settings“ und wechseln Sie dort den „Activation Mode“. Die Kurzadresse und die beiden Schlüssel werden sofort generiert und können herauskopiert werden. Praktisch für alle, die ihren Mikrocontroller in C programmieren: Vor allen Werten gibt es einen Button, der mit „< >“ beschriftet ist. Der schaltet die Ansicht in die C-typische Char-Formatierung um.

Ist bereits ein Sensor in Betrieb, kann man die eingehenden Nachrichten über den Reiter „Data“ beobachten.

Ausprobieren!

Der Einstieg in LoRaWAN ist dank der übersichtlichen Weboberfläche vergleichsweise einfach – zumindest, wenn man die Funktionsweise von LoRa und LoRaWAN kennt. Mit einer Entwicklungsplatine und dem Vorwissen kommen zügig die ersten Pakete im Netzwerk an.

(jam@ct.de) c't

Literatur

[1] Dušan Živadinović, Schrittweise Revolution, 5G krempelt Smartphone, Router, Auto, und Industrieproduktion um, c’t 8/2019, S. 58

Spezifikation: ***ct.de/y5ey***

Bestandteile einer Nachricht im LoRaWAN

Der Inhalt der Nachricht wird mit AES verschlüsselt. Die Integrität der Daten sichert der MIC (Message Integrity Code), der mit dem NwkSKey berechnet wird.