Sprechende Lampen

Einfache Netzwerke für die Hausautomation mit Zigbee

Zigbee macht den Aufbau eines Funknetzes zwischen Lampen und Sensoren einfach. Wenn man weiß, wie Nachrichten von Gerät zu Gerät weitergegeben werden, wird auch die Fehlersuche einfacher.

Von Jan Mahn

Drahtlose Übertragungswege zur Steuerung von Geräten gibt es viele. Einige Hersteller erfinden einfach ihre eigene Protokollbeschreibung auf dem Reißbrett – wie HomeMatic das BidCoS. Andere schließen sich zu einem Herstellerkonsortium zusammen und entwickeln gemeinsam eine Lösung. Ein solches Gemeinschaftsprodukt ist Zigbee, das von der Zigbee Alliance betreut wird. Mit dabei sind Branchengrößen wie Philips, Bosch, Intel oder Texas Instruments. Wer ein Produkt als „Zigbee Certified“ bewerben will und das Logo nutzen möchte, muss Mitglied der Alliance werden und die Einhaltung der Zigbee-Spezifikation von einer der unabhängigen Testeinrichtungen bestätigen lassen.

Gemeinsames Fundament

Zigbee ist eine Spezifikation. Das bedeutet, dass ein Hersteller sich an alle Inhalte des knapp 600 Seiten langen Dokuments halten muss, wenn er sein Produkt später als „Zigbee Certified“ anbieten will. Den Text und alle in diesem Artikel erwähnten Spezifikationen finden Sie über ct.de/yxnm, teilweise ist für den Download die Angabe einer Mail-Adresse erforderlich.

Die Zigbee-Spezifikation basiert wiederum auf einem IEEE-Standard und weicht von diesem nur in Details ab. Das Dokument IEEE 802.15.4 beschreibt die unteren beiden Schichten im OSI-Schichtenmodell zum Aufbau eines „Wireless Personal Area Networks“. Neben dem Frequenzbereich von 2400 bis 2483,5 MHz sieht der Standard noch weitere Bereiche vor, fast alle Zigbee-Geräte arbeiten aber wie WLAN und Bluetooth bei 2,4 GHz. Jedes Gerät bekommt bei der Herstellung eine einmalige physische Adresse, bestehend aus einer 32 Bit langen Herstellerkennung und einer 32 Bit langen Seriennummer (Media Access Control, MAC).

Gerätekunde

In einem Netz nach IEEE 802.15.4 gibt es verschiedene Gerätetypen, die auch in der Zigbee-Spezifikation unter etwas anderem Namen vorkommen. Zentrum ist der Coordinator, der Chef im Netzwerk. Diese Rolle darf es nur einmal geben, er muss permanent laufen und erreichbar sein. Bei der ersten Anmeldung eines neuen Geräts weist der Coordinator jedem Gerät eine 16 Bit lange Adresse zu, die im Netzwerk einmalig ist. Damit ist die theoretische Größe eines Netzwerks auf 65.536 Geräte beschränkt. Der Coordinator selbst hat immer die Adresse 0x0000.

Weitere Geräte, die neben dem Coordinator immer erreichbar sind, nennt der IEEE-Standard „Full Function Device“ – im Zigbee-Netz heißen sie „Router“. Sie können Nachrichten weiterleiten, die nicht an sie selbst adressiert sind, und kommunizieren dazu mit anderen Routern über mögliche Wege durch das Netz. Gefundene Pfade speichern sie in Routingtabellen. Diese Routing-Funktionen sind Teil der dritten OSI-Schicht und werden daher in der Zigbee-Spezifikation beschrieben. Router dürfen zahlreich im Netzwerk vorkommen, es können Maschen- oder Baumstrukturen entstehen.

Geräte, die nicht rund um die Uhr aktiv sind, nennt der Standard „Reduced Function Device“ – bei Zigbee heißen sie

„End Device“. Sie verbringen die meiste Zeit in einem Schlafzustand und erwachen nur für die Übertragung einer Nachricht. Da man sich auf ihre Weiterleitungsfähigkeiten nicht verlassen kann, dürfen sie auch keine Nachrichten weiterleiten. Beispiele sind Fernbedienungen oder Sensoren, die mit Batterien arbeiten.

Gerätepraxis

In der Praxis werden die Aufgaben des Coordinators meist von einem Netzwerk-Gateway des jeweiligen Herstellers übernommen. Sie haben ein Funkmodul für die Zigbee-Anbindung und WLAN oder Ethernet, um sie mit dem Heimnetz zu verbinden. Möchte der Benutzer neue Geräte in das Zigbee-Netzwerk aufnehmen, aktiviert er den Aufnahme-Modus im Coordinator. Das neue Gerät, das sich im Werkszustand befinden muss, bittet um Aufnahme – also um Zuteilung einer netzwerkweiten Adresse – und um den Schlüssel, mit dem der Verkehr zwischen Netzwerkteilnehmern verschlüsselt ist. Die Schlüsselübergabe ist der kritische Moment. Jeder, der während eines Aufnahmevorgangs den Funkverkehr abhört, könnte den Schlüssel mithören und später alle Nachrichten entschlüsseln oder selbst gültige Nachrichten verschicken.

Universalschlüssel

Da fast alle Zigbee-Geräte keine Bedienelemente, kein Display und keine Ressourcen für aufwendige kryptografische Rechenoperationen haben, brauchte man eine Lösung, die etwas sicherer als eine Klartextübertragung des Netzwerkschlüssels ist, dem Benutzer aber keinen Aufwand bereitet. Die Lösung ist ein einheitlicher Master-Key. Den bekommen Hersteller nur, wenn sie Mitglied der Zigbee Alliance werden und sich zur Geheimhaltung verpflichten – seit Jahren findet man ihn allerdings im Internet. Dieser Schlüssel wird nur für die verschlüsselte Übermittlung des Netzwerk-Keys verwendet. Weil man den Schlüsselaustausch also getrost als unsicher bezeichnen kann, gibt es noch eine physische Sicherung: Die Geräte senken während der Aufnahmephase die Sende- und Empfangsleistung und bewerten anhand der Verbindungsqualität, ob das Gegenüber in der Nähe ist. Daher muss der Nutzer seine Zigbee-Glühlampe zum Anlernen direkt neben die Bridge legen.

Ein Angreifer müsste sich also zum richtigen Zeitpunkt, nämlich wenn der Aufnahme-Modus aktiv ist und ein Gerät angelernt wird, am besten in der Wohnung befinden, um den Schlüssel abzuhören. Ist der Netzwerkschlüssel erst mal übertragen, ist Zigbee vergleichsweise sicher. Alle Nachrichten werden mit AES-128 verschlüsselt. Replay-Attacken, also das Aufzeichnen und Abspielen einer Nachricht, werden durch Counter verhindert, die nach einer Nachricht erhöht werden. Doppelte Nachrichten werden verworfen.

Das Zurücksetzen in den Werkszustand lösen die Hersteller unterschiedlich, und der Benutzer muss einen Blick in die Bedienungsanleitung werfen. Einige Geräte brauchen einen Befehl von einer Fernbedienung oder des Coordinators, der auch mit sehr kleiner Sendeleistung verschickt wird. Andere Geräte müssen fünf oder sechs Mal hintereinander an- und ausgeschaltet werden.

Einheitssprache

Nach dem Abschluss der Aufnahmeprozedur können sich Geräte im Netz untereinander über die 16-Bit-Kurzadresse erreichen und Nachrichten schreiben.

Was die Nachrichten enthalten, hängt von der Art des Geräts ab. Damit Zigbee-Produkte auch über Herstellergrenzen miteinander arbeiten können, hat man sich zunächst auf Nutzungsprofile geeinigt. Lampen, Schalter und Licht-Fernbedienungen fielen in das Profil „Zigbee Light Link“. Hier werden Nachrichten für Helligkeit, An/Aus, Farbtemperatur oder Farbmischung spezifiziert. Andere Produkte aus dem vernetzten Zuhause fielen in das „Home Automation Public Application Profile“. Diese Spezifikation listet zum Beispiel Steckdosen, Sensoren, Türschlösser und Heizkörperthermostate und passende Bedienteile auf. Aber auch Lampen konnten nach dieser Spezifikation arbeiten. Für den Anwender war das frustrierend, weil nicht jedes Zigbee-Produkt mit allen Geräten kompatibel war. Abhilfe soll Zigbee 3.0 schaffen, das 2015 spezifiziert wurde. Die Profile wurden zusammengefasst, gleichzeitig ist Zigbee 3.0 abwärtskompatibel zu Light Link und dem Hausautomations-Profil. Seit Anfang 2018 unterstützt die weitverbreitete Hue-Bridge (Version 1 und 2) Zigbee 3.0, IKEAs Trådfri-Lampen sprechen weiter Light Link und bleiben kompatibel.

Probleme lösen

Wie jede Übertragung per Funk ist auch Zigbee anfällig für Störungen. Der Frequenzbereich bei 2,4 GHz ist mit WLAN und Bluetooth schon stark frequentiert. Stört etwas, bringt ein Kanalwechsel auf einen der anderen 25 Kanäle meist Besserung. Optimieren kann man auch den Empfang: Wer alle Ecken seines Hauses mit Zigbee erreichen will, sollte in jedem Raum einen Router platzieren – zum Beispiel in Form eines Leuchtmittels. Der konventionelle Lichtschalter sollte dann aber stillgelegt werden, damit niemand wichtige Knotenpunkte des vermaschten Netzwerks ausknipsen kann. Wer Probleme mit der Steuerung über die App des Herstellers hat oder mit dem Funktionsumfang nicht zufrieden ist, findet auf Seite 164 eine Bridge im Eigenbau. *(jam@ct.de)* c't

Spezifikationen und Standard:
ct.de/yxnm

Zigbee-Netz im Haushalt

Geräte, die ständig mit Strom versorgt werden, können als Router arbeiten und das Signal weiterleiten.