Bild: Andreas Martini

Selbstableser

Heizkostenverteiler, Gas- und Wasserzähler per Funk auslesen

Die Energiepreise steigen aktuell – wie teuer der Winter genau wird, erfahren Mieter von Wohnungen mit Zentralheizung aber erst nach der nächsten Jahresrechnung. Zu besseren Prognosen kommen Sie, wenn Sie die Messwerte abfangen, die die Heizkostenverteiler regelmäßig per Funk an den Auswerter schicken. So schneiden Sie den Funkverkehr mit.

Von Jan Mahn

Die Heizkostenabrechnung, eines der letzten ungelösten Rätsel der Menschheit – so kommt es zumindest Mietern vor, die alljährlich die kleingedruckte Abrechnung in Händen halten. Dabei soll das Verfahren mehr Gerechtigkeit schaffen: Statt die gesamten Heizkosten gleich auf alle Wohnungen oder nach Quadratmetern aufzuteilen, installieren Hausverwaltungen und Vermieter an allen Heizkörpern sogenannte Heizkostenverteiler. Früher nannte man die noch Verdunster, heute arbeiten die Geräte digital: Ausgestattet mit einer Batterie und zwei Temperatursensoren messen die neuen Heizkostenverteiler die Temperatur auf ihrer Innen- und der Außenseite, also am Heizkörper und im Raum. Aus der Temperaturdifferenz ermitteln sie Verbrauchseinheiten.

Am Ende des Jahres kann der Vermieter die Gesamtkosten fürs Heizen im ganzen Haus durch die Anzahl aller von den Geräten gemessenen Einheiten teilen und erhält so einen Preis pro Einheit. Jeder Mieter zahlt dann für die Einheiten seiner Heizkörper. Eigentlich einfacher Dreisatz, aber mit Tücken – diese werden in der Norm DIN EN 834 behandelt (zu finden über ct.de/ys9f). Rechtliche Grundlage für dieses Abrechnungssystem ist die Heizkostenverordnung (HeizkostenV), ebenfalls nachzulesen über ct.de/ys9f.

c't Hardcore

In der ersten Entwicklungsstufe der digitalen Heizkostenverteiler war die einzige Schnittstelle, um an die Messwerte zu kommen, eine einfache einzeilige 7-Segment-Anzeige. Zu einem Stichtag fanden die Mieter entweder den Zettel „Der Ableser kommt. Seien Sie bitte in der nächsten Woche zwischen 7 und 17 Uhr zu Hause“ im Briefkasten, oder mussten mühsam selbst die Werte abschreiben.

Kontaktlos ablesen

Sollten Sie Heizkostenverteiler an Ihren Heizkörpern, aber noch nie Kontakt mit einem Ableser gehabt haben, können die Geräte sich aller Wahrscheinlichkeit nach per Funk artikulieren. Zum Empfang nutzen die Ablesefirmen, die diese Dienstleistung im Auftrag von Hausverwaltungen und Vermietern anbieten, zwei Verfahren: Im einfacheren Fall kommt nach dem Stichtag ein Ableser mit einem mobilen Lesegerät ins Treppenhaus und sammelt dort die gefunkten Werte aller Sensoren ein. Dieses Verfahren heißt bei den Ablesefirmen Walk-by. Alternativ gibt es auch stationäre Gateways, die das ganze Jahr im Treppenhaus oder an anderer zentraler Stelle hängen. Sie sammeln die Messwerte und schicken sie regelmäßig über das Internet an den Auswerter. Seit Oktober 2020 sind fernauslesbare Geräte auch kein Luxus mehr, sondern Pflicht: Gemäß der Energieeffizienzrichtlinie der EU (EED) dürfen nur noch funkende Sensoren neu eingebaut werden, bestehende Altgeräte ohne Funk müssen spätestens am 1. Januar 2027 verschwunden sein.

Das Funken und Fernauswerten ist praktisch für Vermieter und Dienstleister, als Mieter hat man vom Datenschatz dagegen wenig. Dabei wäre es doch schön zu wissen, zu welchen Tages- und Nachtzeiten welcher Heizkörper wie viele Verbrauchseinheiten verursacht und wann es wie warm ist. Mit einer solchen Datengrundlage, anschaulichen Diagrammen und daraus abgeleiteten Sparmaßnahmen ließe sich der Verbrauch optimieren. Ab dem 1. Januar 2022 wird die Rechtslage, ebenfalls im Rahmen der EED, für Mieter zumindest etwas besser: Sie bekommen einen Anspruch auf monatliche Zwischenberichte zum Verbrauch, sofern bereits Funksensoren installiert sind. Das ist besser als eine Jahresabrechung und soll zum Sparen motivieren, ist für private Datenauswertung, systematische Optimierung und Einbindung ins Smart Home aber nicht genug.

Wir fragten bei Techem, einem der großen Anbieter in Deutschland nach, wie Kunden zukünftig an die Daten kommen. Das Walk-by-Verfahren mit Ausleser im Treppenhaus werde zukünftig verschwinden und durch ein Gateway ersetzt. Wenn die Kunden dem Vermieter ihre Mailadresse mitteilen, bekommen sie Zugriff auf einen Onlinedienst für monatliche Übersichten im PDF-Format. Eine kleinteiligere Aufschlüsselung der Daten sei aktuell nicht geplant.

Auf Hilfe von Vermieter und Auslesefirma kann man bei solchen Smart-Home-Extrawünschen nicht vertrauen und muss selbst Hand anlegen – Zeit für etwas Funkprotokollanalyse, einen Raspi und Open-Source-Software. Selbst wenn die eigene Wohnung nicht mit kompatiblen Geräten ausgestattet ist, ist das ein interessanter Ausflug in die Themen Funkübertragung und Datensicherheit im Äther.

Der OMS-Standard

Die Suche nach den verschollenen Messpunkten beginnt im Datenblatt. In zahlreichen Dokumenten unterschiedlicher Hersteller, die wir stichprobenartig ausgewertet haben, fanden wir überall eine Frequenz im Bereich um 868 MHz. Dort darf jeder ohne Anmeldung Daten funken, der Bereich ist für Signale sogenannter „Short Range Devices“ (SRD) reserviert, die im Umkreis von wenigen Dutzend Metern empfangen werden. Die gute Nachricht: Auch wenn die Auslesefirmen in diesem zuteilungsfreien Frequenzbereich funktechnisch alles anstellen könnten, was die Allgemeinzuteilung erlaubt (maximal 25 Milliwatt Sendeleistung, maximal 1 Prozent zeitliche Nutzung pro Gerät), gibt es einen Standard, an dem viele Hersteller von Heizkostenverteilern mitgearbeitet haben und den sie – mit Abweichungen – auch einhalten.

Der gemeinsame Standard heißt Open Metering System (OMS) und Mitglied im Verein „OMS-Group e. V.“ sind unter anderem die großen Ablesefirmen und Hersteller von Geräten wie Itron, Techem oder Qundis. Wenn Sie Ihren Hersteller oder Anbieter in der Mitgliederliste (siehe ct.de/ys9f) finden, stehen die Chancen gut, dass Sie mit überschaubarem Aufwand an die Daten kommen.

OMS definiert nur die Anwendungsschicht und arbeitet mit Funkübertragung über das Verfahren „Wireless M-Bus“ (wM-Bus), beschrieben in der Norm EN 13757-4 (siehe ct.de/ys9f). Und dort sind mehrere Betriebsmodi für unterschiedliche Anwendungsfälle definiert: Auf 868,3 MHz funken Sender in den Modi S1 und S2 mit gemütlichen 32,7 Kbit/s. Das S steht für „stationary“, es wird also ein stationärer Empfänger im Treppenhaus erwartet. Daher senden die Geräte nur einige Male am Tag. Der Modus S1 ist unidirektional, im Modus S2 kann das Gerät nach dem Senden einer Nachricht auf eine Antwort warten. Zum Kodieren der Informationen kommt sogenanntes Manchester-Encoding zum Einsatz (mehr dazu auf S. 30), das so einfach ist, dass es auch günstige und alte Chips beherrschen. Im Gegenzug dauert jede Übertragung mit diesem Verfahren etwas länger, was den Akku der Sender belastet.

Die Modi T1 und T2 (ebenfalls uni- und bidirektional) arbeiten bei 868,95 MHz, hier wird aber keine stationäre Empfangsstation erwartet. Damit der menschliche Ausleser nicht einen ganzen Arbeitstag mit dem mobilen Empfänger im Treppenhaus verbringen muss, bis alle Pakete ins Netz gegangen sind, senden die Geräte hier regelmäßig im Abstand von wenigen Minuten. Teilweise werden die Hersteller hier auch kreativ, um die Batterie zu schonen. In den Datenblättern fanden wir zum Beispiel bei Qundis einen Betriebsmodus, in dem nur zwischen 8 und 18 Uhr regelmäßig gesendet wird.

Die von OMS bevorzugten und als zukunftsfest markierten Modi heißen C1 und C2 (für „compact“) bei 868,95 MHz. Dort funken die Geräte mit zügigen 100 Kbit/s und nutzen das Verfahren „Non-Return to Zero“ (NRZ).

Wie die Daten aussehen, beschreibt OMS in mehreren Dokumenten und liefert auch ausführliche Beispiele (siehe ct.de/ys9f). Jede Nachricht beginnt mit Metadaten, dem „Data Link Layer“. In 10 Bytes übertragen die Geräte unter anderem einen Code für den Hersteller, ihre ID in Form einer achtstelligen Dezimalzahl und ihren

Was tun bei Fußbodenheizungen?

Heizkostenverteiler sind kein Allheilmittel für alle Situationen, sondern nur für den klassischen Heizkörper an der Wand gedacht. Bei Fußbodenheizungen funktionieren sie zum Beispiel nicht, und auch bei kombinierten Heiz- und Kühlsystemen sind sie machtlos und nicht zugelassen. Für solche Fälle gibt es Wärme- und Kältezähler und auch kombinierte Zähler, die in den Kreislauf eingebaut werden und messen, was an ihren Fühlern vorbeifließt. Was dieser Artikel für die am weitesten verbreiteten Heizkostenverteiler beschreibt, gilt auch für viele solcher Geräte: Auch sie funken ihre Messwerte und nutzen häufig denselben Übertragungsstandard.

```
version: "3.8"
services:
  wmbusmeters:
    image: weetmuts/↵
↳wmbusmeters:latest-armhf
    container_name: wmbusmeters
    restart: always
    privileged: true
    volumes:
      - ./data:/wmbusmeters_data
      - /etc/localtime:/etc/↵
↳localtime:ro
      - /dev/:/dev/
```

Wmbusmeters hat zahlreiche Abhängigkeiten, die man alle selbst kompilieren müsste. Mit einer Docker-Compose-Zusammenstellung sparen Sie sich den Aufwand.

Typ. Ein Heizkostenverteiler meldet sich zum Beispiel gemäß OMS-Spezifikation mit dem Code `08h`, Wasserzählern ist der Code `07h` zugeteilt. Zentraler Teil aller Nachrichten ist der „Application Layer“, der die Nutzdaten enthält. Hier gibt es die erste schlechte Nachricht für alle, die die Daten gern abfangen und selbst nutzen möchten: Es ist möglich, aber nicht verpflichtend, die Nutzdaten mit AES-128 symmetrisch zu verschlüsseln. Das ist nicht mehr der letzte Schrei, aber noch immer so sicher, dass Sie keine Chance haben, an die Daten zu kommen, wenn Ihr Anbieter verschlüsselt und Ihnen den Schlüssel nicht überlässt.

Inhaltlich sind, je nach Messgerät, sehr viele Spezialfälle für Datenpakete spezifiziert – für Heizkostenverteiler relevant sind die verbrauchten Einheiten ab einem Stichtag (und das Datum des Stichtags). Auch historische Werte (zum Beispiel für die letzten Monate) können übertragen werden. Zusätzlich können die Hersteller weitere Daten übertragen – einige Heizkostenverteiler schicken zum Beispiel die aktuell gemessenen Temperaturen mit, für die eigene Auswertung ist das ein Geschenk.

Funk auswerten

Mit diesem Wissen könnten Sie sich jetzt an die Analyse der Datenpakete Ihrer Sensoren machen – angesichts der vielen möglichen Daten, die in den Geräten stecken können, ist aber einiges an Erfahrung und Reverse-Engineering-Arbeit nötig, um verwertbare Daten aus den Paketen zu ziehen.

Dankenswerterweise haben andere schon Vorarbeit geleistet. Bereits seit 2017 arbeitet der Entwickler Fredrik Öhrström an der kleinen Software Wmbusmeters, die S1-, T1- und C1-Telegramme von OMS-Sendern auswertet und als JSON-Objekte zurückgibt. Zusammen mit einer wachsenden internationalen Community, die ihn mit Datentelegrammen verschiedener Sensoren versorgt, hat er Übersetzer für viele Geräte in die Software eingebaut. Darunter sind auch die Heizkostenverteiler, Wasseruhren und Wärmezähler der großen deutschen Anbieter.

Verschiedene Empfänger-Hardware kommt für die 868-MHz-Signale infrage und wird von Wmbusmeters unterstützt. Beste Wahl aus unserer Sicht sind Sticks mit dem Chip RTL2832U, die unter dem Namen RTL-SDR mit Antenne ab 45 Euro auf Handelsplattform von deutschen Händlern angeboten werden. Der Stick ist extrem vielseitig und eignet sich für viele spannende Funkexperimente und den Einstieg ins Radio-Hacking [1].

Unter Windows und macOS bekamen wir Wmbusmeters nicht ohne Ruckeln und viel Handarbeit zum Laufen. Zügig ging es unter Linux – zum Beispiel auf einem Raspi, der problemlos nebenbei noch andere Smart-Home-Aufgaben erledigen kann. Installieren Sie eine aktuelle Version von Raspberry Pi OS und verbinden sich per SSH.

Damit Sie Wmbusmeters und die diversen Abhängigkeiten nicht alle nacheinander selbst kompilieren müssen, empfehlen wir den Betrieb in einem Docker-Container. Wie Sie Docker und Docker-Compose auf dem Raspi zum Laufen bekommen, erfahren Sie in einem kostenlosen und regelmäßig aktualisierten Online-Artikel, zu finden über ct.de/ys9f.

Legen Sie zu Beginn einen neuen Ordner für das Projekt an und springen Sie dort hinein:

```
mkdir scan
cd scan
```

Alle folgenden Kommandozeilenbefehle gehen davon aus, dass Sie in diesen Ordner navigiert sind. Erstellen Sie dort eine Datei mit dem Namen docker-compose.yaml und fügen Sie die Struktur aus dem Kasten links oben ein. Dem Container wird darin der Ordner data im aktuellen Verzeichnis übergeben – Docker legt den für Sie an, wenn Sie die Zusammenstellung starten. Darin landen Konfiguration und die gelesenen Daten.

Schließen Sie Ihren RTL-SDR-Stick mit Antenne an und starten Sie den Container mit

```
docker compose up -d
```

Meldet Docker Vollzug, beginnt schon die Observation des Funkspektrums. Wmbusmeters erkennt den Stick automatisch und beginnt, im Modus T1 zu lauschen. Einer der Vorteile des RTL-SDR-Sticks: Mit ihm können Sie mehrere Modi parallel betreiben. Öffnen Sie dafür die Konfigurationsdatei:

```
sudo nano data/etc/wmbusmeters.conf
```

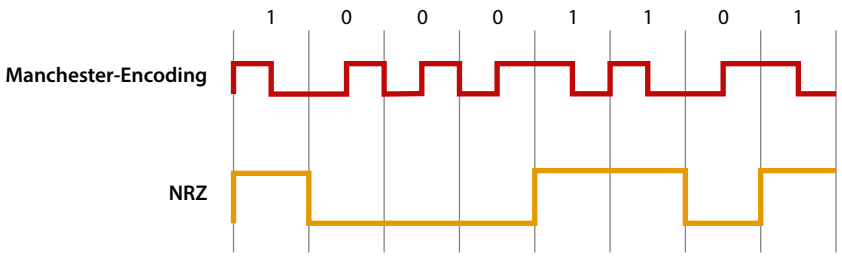
Passen Sie dort die mit `listento` beginnende Zeile wie folgt an:

```
listento=c1,t1,s1
```

Speichern Sie die Änderung und starten Wmbusmeters mit `docker compose restart`

Manchester-Encoding und NRZ

Einsen und Nullen der Daten müssen zur Übertragung kodiert werden. Beim Manchester-Encoding besteht das Bit 1 aus einem High-Signal, gefolgt von einem Low-Signal. Eine 0 wird über ein Low-Signal, gefolgt von einem High-Signal kodiert. Der Vorteil: Der Empfänger weiß genau, wie lang ein Bit ist. Das Verfahren „Non-Return to Zero“ (NRZ) ist effizienter, dafür können lange Signalberge und Täler aufeinander folgen – Empfangsprobleme sind wahrscheinlicher.



neu. So können Sie immer verfahren, wenn Sie Änderungen an der Konfiguration vornehmen.

Um live dabei zu sein, wenn Wmbusmeters Daten empfängt, beobachten Sie mit dem Befehl `tail` die Log-Datei:

```
tail -f data/logs/wmbusmeters.log
```

Mit dem Parameter `-f` wird die Kommandozeile blockiert und Sie sehen Änderungen sofort (mit Strg+C beenden Sie den Modus). Wenn alles nach Plan läuft, sehen Sie irgendwann Einträge wie folgenden:

```
Received telegram from: 12341111
  manufacturer: (TCH) Techem (0x5068)
  type: Heat Cost Allocator (0x80)
  ver: 0x69
  device: rtlwmbus[00000001]
  rssi: 43 dBm
  driver: fhkvdataiii
```

Wie lange sich das Warten lohnt, hängt vom Sendezyklus Ihrer Geräte ab – verzweifeln Sie also nicht und lassen den Raspi bei Bedarf 24 Stunden laufen. In der Wohnung, die wir zum Test auserkoren hatten, purzelten neue Nachrichten im Sekundentakt hinein. In der Wohnung selbst sind sieben Geräte von Techem installiert, insgesamt empfingen wir Daten von 25 verschiedenen Sendern. Die achtstellige ID steht im Log immer in der ersten Zeile. Sofern in der letzten Zeile ein `driver` zu finden ist, wird das Gerät von Wmbusmeters unterstützt. Bevor es weitergeht, müssen Sie die IDs Ihrer Geräte zusammentragen. Halten Sie Ausschau nach achtstelligen Zahlen – im Display, aufgedruckt, oder auf der letzten Heizkostenabrechnung. Bei uns war ein System zu erkennen, die ersten vier Stellen waren für alle Geräte der Wohnung identisch. Jetzt können Sie Ihre IDs gezielt abonnieren. Erstellen und bearbeiten Sie dafür eine Konfigurationsdatei:

```
sudo nano data/etc/wmbusmeters.d/heat
```

Wie die Datei heißt, ist Ihnen überlassen. Sie können für jeden Heizkörper eine eigene Datei anlegen oder mehrere in einer Datei abfragen. Fügen Sie darin folgende Zeilen ein:

```
name=bathroom
id=12341111
key=NOKEY
driver=auto
```

Wenn Sie eine Datei pro Heizkörper anlegen wollen, vergeben Sie einen sprechenden Namen (`name`) und geben die ID (`id`) an. Sollte auch Ihr Anbieter ein Muster für all Ihre Geräte verwenden, können Sie mit dem Wildcard-Symbol `*` arbeiten und zum Beispiel schreiben:

```
id=1234*
```

Die Angabe von `driver` ist optional, statt `auto` könnten Sie auch den Treibernamen angeben, den Sie in den Logs gesehen haben. Speichern Sie die Datei (oder je eine pro Heizung) und starten anschließend mit `docker compose restart` neu. Jetzt wird es spannend: Sofern Ihre Geräte unverschlüsselt senden, finden Sie ab jetzt JSON-Daten im Ordner data/logs/meter_readings, für jede Konfigurationsdatei eine Datendatei. Bekommen Sie nur Datensalat, verschlüsseln Ihre Geräte – probieren Sie gern, Ihren Anbieter nach dem Schlüssel zu fragen. Viel Hoffnung können wir Ihnen leider nicht machen.

In der Standardeinstellung werden die Daten mit jedem neuen Paket überschrieben. Um das Verhalten zu ändern, öffnen Sie wieder die Konfigurationsdatei in data/etc/wmbusmeters.conf und ändern die vorletzte Zeile in

```
meterfilesaction=append
```

Was Sie mit den Daten anstellen, ist Ihrer Kreativität überlassen. Wenn Sie schon einen Smart-Home-Server mit einem MQTT-Broker betreiben, reicht eine Zeile in der Konfigurationsdatei, um jedes Datenpaket per MQTT zur weiteren Auswertung zu verschicken. Sie könnten die Daten auf diesem Weg auffangen, speichern und Diagramme zeichnen. Tragen Sie einfach folgende Zeile ein (ändern Sie dabei die IP Ihres MQTT-Brokers):

```
shell=/usr/bin/mosquitto_pub -h ↵
↳<IP> -t wmbusmeters/$METER_ID -m ↵
↳"$METER_JSON"
```

Jemand zu Hause?

Dass die Daten bei uns unverschlüsselt verschickt werden, kann man positiv sehen und die Daten für die eigene Auswertung nutzen. Man kann es aber auch zum Datenschutzproblem erklären – schließlich könnten wir jetzt auch für unsere Nachbarn im selben und im Nachbarhaus Heizprofile erstellen. Wie hoch der Anteil an unverschlüsselten Datenpaketen in der ganzen Republik ist, können wir angesichts der vielen, teilweise lokal operierenden Anbieter unmöglich einschätzen. Wenn Sie die Anleitung in diesem Artikel erfolgreich nachstellen konnten, freuen wir uns daher über eine Rückmeldung per Mail.

Auf Anfrage teilte uns Techem mit, dass die Heizkostenverteiler neuerer Generation, wie auf der Homepage versprochen, per AES verschlüsseln und die alten irgendwann ausgetauscht werden. Außerdem bot man uns an, neue Geräte einzubauen – für die gerade beginnende Heizperiode verzichten wir dankend und sammeln die im Dreiminutentakt anfallenden Daten in unserer Datenbank [2].

(jam@ct.de) c't

Literatur

[1] Andrijan Möcker, Lauschposten, Raspi als Funkempfänger-Server, c't 23/2019, S. 30

[2] Jan Mahn, Geschichtsschreiber, InfluxDB: Spezialisierte Datenbank für Messwerte und Logging, c't 5/2019, S. 154

Spezifikationen: ***ct.de/ys9f***

Für Sparfüchse: Der Registrierbeginn

Seit es Verdunster an Heizungen gibt, existieren auch Tricks zur Manipulation durch Abbauen, Einfrieren und Abdecken. Doch solche Versuche sind illegal und in Zeiten von digitalen Heizkostenverteilern nicht mehr so einfach.

Sparen kann man aber auch legal, wenn man das Datenblatt der eigenen Zähler aufmerksam liest. Im Datenblatt der Heizkostenverteiler, mit denen wir die Anleitungen für diesen Artikel ausprobiert haben, fanden wir den Hinweis auf den sogenannten „Registrierbeginn", also den Schwellwert, ab dem überhaupt Einheiten berechnet werden. Demnach beginnt die Zählung bei diesen Geräten erst, wenn die Heizfläche 22,5 °C erreicht und die Heiztemperatur 4 Grad über Raumtemperatur liegt. Auf Stufe 1 des Thermostatventils wurden diese Schwellwerte bei uns nicht erreicht – einen Flur konnten wir also mit moderatem Heizen vorm totalen Auskühlen bewahren, ohne dass Einheiten berechnet wurden.