IoT-Protokolle und Konnektivität: Wie Dinge miteinander sprechen

Vom Smart Home bis zur Smart City – ein verständlicher Überblick

Klaus Quibeldey-Cirkel

26. Januar 2026

Zusammenfassung

Vom Bodenfeuchtesensor bis zur Fabrikautomation: IoT-Geräte haben völlig unterschiedliche Anforderungen an Reichweite, Energieverbrauch und Reaktionszeit. Dieser Artikel zeigt, warum es im Internet der Dinge kein universelles „Ein-Protokoll-Netz“ gibt, wie MQTT und CoAP Daten austauschen, welche Funktechnologien (Thread, Wi-Fi, LoRaWAN, NB-IoT, 5G RedCap) wofür geeignet sind – und wie Standards wie Matter Interoperabilität und Sicherheit verbessern.

1 Warum IoT-Kommunikation komplizierter ist als „WLAN an, fertig“

Im Alltag wirkt Vernetzung simpel: Smartphone ins WLAN, App öffnen, fertig. Im *Internet der Dinge* (IoT) sieht die Realität anders aus. Weltweit sind bereits über 20 Milliarden IoT-Geräte im Einsatz [1] – und sie könnten unterschiedlicher kaum sein: Ein Bodenfeuchtesensor soll zehn Jahre mit einer Batterie auskommen und nur alle paar Stunden einen Messwert senden. Ein fahrerloses Transportsystem in einer Fabrik braucht dagegen millisekundenschnelle Reaktionen und mitunter genug Bandbreite für Kameradaten.

Diese Spannweite führt zu einer unbequemen Wahrheit: Es gibt nicht *das* IoT-Protokoll und nicht *die* perfekte Funktechnik. Stattdessen muss man sich wie bei Werkzeugen entscheiden: Hammer, Schraubendreher, Zange – jedes ist gut, aber eben für etwas anderes.

Das IoT-Trilemma

Hohe Reichweite, hohe Datenrate und lange Batterielaufzeit lassen sich nicht gleichzeitig maximieren. Jede Konnektivitätstechnologie macht Kompromisse – und genau das ist im IoT normal.

2 Ein Stack statt eines Standards

Wenn Geräte „miteinander sprechen“, passiert das in Schichten: Oben wird festgelegt, *wie* Daten beschrieben und ausgetauscht werden (z. B. Messwerte, Befehle, Zustandsänderungen). Unten entscheidet die Konnektivität, *wie* diese Bits überhaupt von A nach B kommen (WLAN, Mesh-Funk, Mobilfunk, LPWAN).

In der Praxis hilft eine grobe Einteilung:

- **Anwendungsebene:** Protokolle wie MQTT oder CoAP regeln Nachrichten, Topics, Ressourcen und Zustelllogik.
- **Lokale Netze:** Thread, Zigbee, Bluetooth LE oder Wi-Fi verbinden Geräte im Haus, Büro oder in der Halle.
- **Weitbereich:** LoRaWAN, NB-IoT, LTE-M oder 5G verbinden Sensoren über Kilometer und Städte hinweg.

3 Oben im Stack: MQTT und CoAP

3.1 MQTT: Wenn viele zuhören sollen

MQTT ist im IoT so etwas wie der „Postverteiler“. Geräte senden nicht an konkrete Empfänger, sondern an *Topics* (Themenpfade). Eine zentrale Instanz, der *Broker*, verteilt diese Nachrichten an alle Abonnenten. Das ist besonders praktisch, wenn viele Systeme dieselben Daten benötigen: Dashboard, Alarmierung, Datenbank und Analyse können parallel abonnieren, ohne dass der Sensor sie alle kennen muss.

Die Analyse der Bandbreitennutzung zeigt, dass MQTT zwar auf TCP aufsetzt – was einen gewissen Overhead für den Verbindungsaufbau (Drei-Wege-Handshake) mit sich bringt –, aber in Szenarien mit stabilen, langlebigen Verbindungen extrem effizient ist. Sobald die TCP-Verbindung steht, ist der Overhead pro Nachricht minimal. Studien bestätigen, dass MQTT in Umgebungen mit geringer Paketverlustrate eine geringere Latenz aufweist als konkurrierende UDP-basierte Protokolle, da der TCP-Stack auf Kernel-Ebene die Flusskontrolle effizienter handhabt als Application-Layer-Implementierungen [2].

Ein wichtiges Detail: MQTT kann die Zustellgarantie fein abstufen [3]:

- **QoS 0:** schnell, aber ohne Bestätigung („Fire-and-Forget“).
- **QoS 1:** kommt an, kann aber doppelt ankommen.
- **QoS 2:** kommt genau einmal an, kostet dafür mehr Overhead.

Mit MQTT 5.0 kamen außerdem Funktionen hinzu, die moderne Cloud-Architekturen erleichtern (z. B. Load-Balancing über „Shared Subscriptions“ oder Request/Response-Muster) [3]. Für sehr kleine Sensornetze gibt es MQTT-SN, das die MQTT-Idee auf UDP überträgt und Topic-Namen über kurze IDs schlanker macht [4].

3.2 CoAP: HTTP, aber für Mikrocontroller

Während MQTT eine eigene Nachrichtenwelt baut, folgt CoAP dem Web-Prinzip: Ressourcen haben URIs, und man arbeitet mit GET/PUT/POST/DELETE – ähnlich wie bei HTTP, nur deutlich kompakter und typischerweise über UDP [5].

CoAP kann trotzdem zuverlässig sein: Nachrichten können als *confirmable* markiert werden, dann bestätigt der Empfänger den Erhalt. Und weil permanentes Polling Batterie frisst, gibt es *Observe*: Statt immer wieder nachzufragen, „abonniert“ man eine Ressource und bekommt Updates bei Änderungen [6]. Für größere Daten (z. B. Firmware-Updates) unterstützt CoAP *Block-wise Transfer*, um große Pakete in handliche Stücke zu teilen. Sicherheit läuft meist über DTLS (das TLS-Pendant für UDP).

	MQTT	**CoAP**
Grundidee	Publish/Subscribe über Broker	REST über UDP
Stärken	Telemetrie an viele Empfänger,gutes Ecosystem	kurze „Wake-up-and-send“-Kommunikation, Web-nah
Typische Rolle	Datenstrom ins Backend/Cloud	Geräte-API im lokalen Netz
Sicherheit	meist TLS	meist DTLS

Tabelle 1: MQTT und CoAP im vereinfachten Vergleich

Eine gute Erinnerung daran, dass diese Entscheidung nicht nur „Geschmackssache“ ist, liefern Messstudien, die Latenz, Durchsatz und Energieverbrauch auch unter aktivierter Transportverschlüsselung vergleichen [2].

Faustregel: Welches Protokoll wann?

Viele Datenpunkte, viele Abnehmer, zentrale Verarbeitung: eher MQTT. Sehr seltene Nachrichten, viel Schlafmodus, „Ressource abfragen/-setzen“: eher CoAP. In der Praxis werden beide oft kombiniert.

4 Nahbereich: Zigbee, Thread, BLE und Wi-Fi

4.1 Zigbee vs. Thread: Zwei Mesh-Welten auf ähnlichem Funk

Zigbee und Thread funken häufig auf derselben physikalischen Basis (IEEE 802.15.4), unterscheiden sich aber in der Philosophie: Zigbee ist historisch ein „eigener Stack“ ohne natives IP. Deshalb braucht es fast immer einen Hub, der zwischen Zigbee-Welt und IP-Welt übersetzt. Dazu kam lange eine gewisse Fragmentierung zwischen Profilen und Hersteller-Ökosystemen [7].

Thread setzt dagegen auf IPv6 über 6LoWPAN: Jedes Gerät ist direkt im IP-Adressraum, und der *Border Router* routet IP-Pakete statt Anwendungsdaten zu übersetzen. Seit Thread 1.4 können Border Router verschiedener Hersteller leichter in einem gemeinsamen Mesh zusammenarbeiten (Credential Sharing) [8]. Genau diese IP-Nähe macht Thread zu einem wichtigen Fundament für moderne Smart-Home-Standards wie Matter.

4.2 Bluetooth LE Mesh: Stark beim „Handshake“, schwächer bei großen Netzen

Bluetooth LE ist überall, weil jedes Smartphone es kann. Für IoT-Netze ist BLE Mesh interessant, das Nachrichten per *Managed Flooding* im Netz weiterreicht. Das funktioniert gut für kleine bis mittlere Installationen und einfache Befehle (Licht an/aus). Bei sehr vielen Geräten und viel Telemetrie skaliert Flooding jedoch schlechter als klassisches Routing, weil redundante Weiterleitungen Bandbreite kosten [9].

4.3 Wi-Fi 6/7: Weniger „Stromfresser“ als früher

WLAN galt lange als zu energiehungrig für Batteriegeräte. Mit Wi-Fi 6 wurde aber u. a. *Target Wake Time* (TWT) populär: Access Point und Gerät handeln Schlaf-/Aufwachzeiten aus, das Funkmodul kann dazwischen länger aus sein. Das macht WLAN für mehr IoT-Geräteklassen attraktiv – besonders dort, wo ohnehin schon ein gutes Wi-Fi-Netz existiert [1].

5 Weitbereich: LoRaWAN, NB-IoT und 5G RedCap

5.1 LoRaWAN: Kilometerreichweite im freien Spektrum

LoRaWAN nutzt unlizenziertes Sub-GHz-Spektrum und erreicht mit robuster Modulation große Reichweiten bei kleinen Datenraten. Typisch ist eine Stern-Architektur: Endgeräte senden an Gateways, die weiter ins IP-Netz routen. Ein praktischer Vorteil: Man kann private Netze aufbauen, ohne Mobilfunkverträge

Technologie	Reichweite	Tempo	Typische Einsätze
Thread (Mesh)	Haus/Etage	250 kbps, <100 ms	Sensoren/Aktoren im Smart Home, Matter-Geräte
Wi-Fi 6 (TWT)	Gebäude	>100 Mbps, <10 ms	Kameras, Türsprechanlagen, „direkt in die Cloud“
LoRaWAN	10–15 km	kbps, s–min	Smart City Metering, Agrar-Sensorik, lange Batterielaufzeit
NB-IoT	Mobilfunkzelle	<250 kbps, 1,5–10 s	Smart Meter,Deep Indoor,Provider-gestützte Abdeckung
LTE-M	Mobilfunkzelle	~1 Mbps, 50–100 ms	Mobile Sensorik, Asset Tracking, Wearables
5G RedCap	Mobilfunkzelle	85–150 Mbps, 10–20 ms	Video, industrielle Telematik, mid-tier IoT

Tabelle 2: Spickzettel: Konnektivität im IoT (Stand 2026, stark gerundet), in Anlehnung an [7]

pro Gerät [10]. Für abgelegene Regionen wird zudem Satelliten-IoT relevanter, etwa durch neue LoRa-Varianten.

5.2 NB-IoT und LTE-M: Mobilfunk für kleine Daten

NB-IoT ist ein 3GPP-Standard im lizenzierten Mobilfunkspektrum. Er spielt seine Stärke dort aus, wo Gebäudedurchdringung, planbare Abdeckung und Provider-Infrastruktur zählen. Stromsparmodi wie PSM und eDRX erlauben lange Schlafphasen. LTE-M ist die mobilere, oft latenzärmere Schwester mit höheren Datenraten – nützlich z. B. für Asset Tracking und Wearables.

5.3 5G RedCap: Zwischen LPWAN und „vollem 5G“

Nicht jedes IoT-Gerät braucht Gigabit, aber manche brauchen mehr als LPWAN. 5G RedCap (Release 17) zielt genau auf diese Mitte: weniger Bandbreite und Hardware-Komplexität als klassisches 5G, aber deutlich mehr Leistung als NB-IoT. Typisch sind etwa 85–150 Mbps und 10–20 ms Latenz [11]. Mit eRedCap (Release 18) wird die Klasse weiter nach unten erweitert (z. B. 5 MHz Bandbreite, ~10 Mbps) [12].

6 Interoperabilität: Raus aus dem Fragmentierungs-Dschungel

6.1 Matter: Ein gemeinsames Smart-Home-Vokabular

Im Smart Home waren Geräte lange in „Walled Gardens“ gefangen: Lampen, Sensoren und Lautsprecher funktionierten nur in bestimmten Apps oder über bestimmte Hubs. Matter soll das aufbrechen, indem es ein gemeinsames Datenmodell und Interaktionsregeln auf IP-Basis definiert – unabhängig davon, ob ein Gerät per Wi-Fi, Thread oder Ethernet verbunden ist. Ein wichtiger Punkt: Matter setzt stark auf lokale Steuerung, Cloud ist optional. Das reduziert Latenz und verbessert Privatsphäre. Neuere Versionen (z. B. 1.4) erweitern das Modell u. a. um Energiemanagement im Haushalt [13].

6.2 Industrie: OPC UA FX vs. MQTT Sparkplug

In der Industrie treffen IT-Welt und Maschinenwelt aufeinander. Zwei Ansätze stehen exemplarisch:

- **OPC UA FX** erweitert OPC UA um deterministische Kommunikation bis in die Feldebene (u. a. über TSN) und bietet ein reiches semantisches Modell.
- **MQTT Sparkplug B** standardisiert Payload und Topic-Struktur für MQTT und passt gut zur Idee eines *Unified Namespace*: Alle Maschinenzustände fließen in einen zentralen Broker, den verschiedene Systeme nutzen können [14].

Welche Strategie besser ist, hängt stark davon ab, ob man primär Echtzeit/Determinismus (Automatisierung) oder Skalierung/Integration (IT) priorisiert.

7 Sicherheit: Klein, aber nicht schutzlos

IoT ist sicherheitskritisch, weil Angriffe nicht nur Daten stehlen, sondern physische Prozesse beeinflussen können. Lange waren viele Geräte zu schwach für etablierte Kryptographie. Genau hier setzen neue Standards an: Das NIST hat 2025 mit Ascon einen Lightweight-Crypto-Standard finalisiert, der für kleine Mikrocontroller optimiert ist [15].

Mini-Checkliste für sichere IoT-Systeme

- Geräteidentität statt „Default-Passwort“: Zertifikate (z. B. X.509) und sichere Schlüsselspeicher (Secure Element).
- Zero-Trust-Denken: jedes Gerät authentifiziert sich, jedes Netzwerksegment wird als potenziell unsicher behandelt.
- Updates einplanen: sichere OTA-Mechanismen sind kein „Nice-to-have“.

8 Fazit: Die richtige Verbindung ist eine Designentscheidung

Die IoT-Landschaft konsolidiert sich, aber nicht auf einen Standard, sondern auf ein Zusammenspiel: IP

wird zum gemeinsamen Nenner, und darüber entscheiden Anwendungsschicht-Standards wie Matter oder industrielle Profile, *wie* Geräte Daten austauschen. Gleichzeitig bleibt die Physik der Gegenpol: Reichweite, Bandbreite und Energieverbrauch erzwingen Kompromisse.

Der Blick nach vorn geht in zwei Richtungen: mehr *Intelligenz am Rand* (TinyML), um Daten gar nicht erst senden zu müssen – und mehr *globale Konnektivität* durch die Verbindung von terrestrischen Netzen und Satelliten-IoT. Wer heute IoT-Systeme plant, plant deshalb nicht nur „Funk“, sondern eine Architektur.

Glossar

5G RedCap Reduced Capability 5G – 5G-Unterprofil für IoT-Geräte mit reduzierten Anforderungen (Energie/Kosten).

AMQP Advanced Message Queuing Protocol – ein zuverlässiges, broker-basiertes Messaging-Protokoll.

BLE Mesh Erweiterung von Bluetooth LE für Mesh-Netzwerke.

Bluetooth LE Bluetooth Low Energy – energiesparsamer Bluetooth-Modus.

Broker In Publish/Subscribe-Architekturen (z. B. MQTT) die zentrale Komponente, die Nachrichten verteilt.

CoAP Constrained Application Protocol – leichtgewichtiges HTTP-ähnliches Protokoll für ressourcenbeschränkte Geräte (UDP).

DTLS/TLS Datagram/TLS – Sicherheitsprotokolle für verschlüsselte Verbindungen (DTLS für UDP, TLS für TCP).

Gateway Vermittler zwischen verschiedenen Netzwerken oder Protokollen (z. B. LoRaWAN → IP).

HTTP/REST Hypertext Transfer Protocol / Representational State Transfer.

Interoperabilität Fähigkeit verschiedener Systeme/Protokolle, zusammenzuarbeiten und Daten semantisch zu verstehen.

Latency Verzögerung zwischen Sende- und Empfangszeitpunkt; kritisch für Echtzeitanforderungen.

LoRaWAN Low Power Wide Area Network – LPWAN für große Reichweiten bei geringem Energieverbrauch.

LTE-M LTE-Machine (eMTC) – mobilfunkbasierte Option für IoT.

LwM2M Lightweight M2M – OMA-Protokoll für Geräte-Management und Telemetrie.

Matter Interoperabilitätsstandard für Smart-Home-Geräte; baut auf Thread, Wi-Fi und IP auf.

Mesh/Star/Tree Netzwerktopologien: Mesh, Star, Tree.

MQTT Message Queuing Telemetry Transport – Publish/Subscribe-Protokoll mit geringem Overhead.

MQTT-SN MQTT for Sensor Networks – Variante für Netzwerktypen ohne TCP/IP.

NB-IoT NarrowBand-IoT – Mobilfunkbasiertes LPWAN.

OPC UA Open Platform Communications Unified Architecture – Industriekommunikation mit Semantik.

OTA Over-The-Air Updates – Aktualisierung von Firmware/Software per Funkverbindung.

Provisioning Prozess, Geräte sicher in ein Netzwerk aufzunehmen.

Publish/Subscribe Kommunikationsmuster: Publisher senden an Topics, Subscriber empfangen relevante Topics über einen Broker.

QoS Quality of Service – Mechanismen zur Sicherstellung von Zustellgarantien.

RESTful Beschreibung von Web-APIs, die HTTP-Methoden konsistent nutzen.

Thread IPv6-basiertes Mesh-Protokoll für drahtlose Heimnetzwerke.

Throughput Datendurchsatz einer Verbindung oder eines Systems.

Wi-Fi Drahtlosnetzwerkstandard für hohe Datenraten.

Zigbee Drahtloses Mesh-Protokoll für Hausautomation.

Z-Wave Proprietäres Funksystem für Hausautomation.

Quellen und weiterführende Literatur

[1] *State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally.* IoT Analytics. 2025. URL: https://iot-analytics.com/number-connected-iot-devices/ (besucht am 26. 01. 2026) (siehe S. 1, 2).

[2] P. A. Seoane u. a. „Performance evaluation of CoAP and MQTT with security support for IoT environments“. In: *Computer Networks* 191 (2021), S. 107996 (siehe S. 1, 2).

[3] *MQTT Version 5.0.* OASIS. 2019. URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (besucht am 26. 01. 2026) (siehe S. 1, 2).

[4] *MQTT-SN Version 1.2.* OASIS. URL: https://docs.oasis-open.org/mqtt-sn/mqtt-sn/v1.2/mqtt-sn-v1.2.html (besucht am 26. 01. 2026) (siehe S. 2).

[5] Zach Shelby, Klaus Hartke und Carsten Bormann. *The Constrained Application Protocol (CoAP).* RFC 7252. IETF, 2014. URL: https://www.rfc-editor.org/rfc/rfc7252 (besucht am 26. 01. 2026) (siehe S. 2).

[6] Klaus Hartke. *Observing Resources in the Constrained Application Protocol (CoAP).* RFC 7641. IETF, 2015. URL: https://www.rfc-editor.org/rfc/rfc7641 (besucht am 26. 01. 2026) (siehe S. 2).

[7] Uniconverge Technologies. *IoT Communication Protocols: LoRaWAN Dominates 2025.* 2025. URL: https://www.uniconvergetech.in/blog/iot-communication-protocols-lorawan/ (besucht am 26. 01. 2026) (siehe S. 2, 3).

[8] *Thread 1.4 Features White Paper.* Thread Group. 2024. URL: https://www.threadgroup.org/Portals/0/Documents/Thread_1.4_Features_White_Paper_September_2024.pdf (besucht am 26. 01. 2026) (siehe S. 2).

[9] *Benchmarking Bluetooth Mesh, Thread, and Zigbee Network Performance.* Silicon Labs. URL: https://www.silabs.com/wireless/multiprotocol/mesh-performance (besucht am 26. 01. 2026) (siehe S. 2).

[10] *NB-IoT vs LoRaWAN: A Comparison of the Two IoT Technologies.* Lansitec. URL: https://www.lansitec.com/blogs/nb-iot-vs-lorawan-a-comparison-of-the-two-iot-technologies/ (besucht am 26. 01. 2026) (siehe S. 3).

[11] *5G RedCap: Benefits, Use Cases and Deployment Considerations.* floLIVE. 2025. URL: https://flolive.net/blog/glossary/5g-redcap-benefits-use-cases-and-deployment-considerations-2025/ (besucht am 26. 01. 2026) (siehe S. 3).

[12] *Filling a Gap? Performance Comparison of RedCap and eRedCap for Mid-Tier Applications.* TU Dortmund University. 2025. URL: https://cni.etit.tu-dortmund.de/storages/cni-etit/r/Research/Publications/2025/Joerke_2025_GLOBECOM/Joerke_GLOBECOM2025_AuthorsVersion.pdf (besucht am 26. 01. 2026) (siehe S. 3).

[13] *Matter 1.4 Enables More Capable Smart Homes.* Connectivity Standards Alliance. URL: https://csa-iot.org/newsroom/matter-1-4-enables-more-capable-smart-homes/ (besucht am 26. 01. 2026) (siehe S. 3).

[14] *Choosing Between MQTT and OPC UA for Smart Automation and Manufacturing.* Balluff. URL: https://www.balluff.com/en-us/blog/choosing-between-mqtt-and-opc-ua-for-smart-automation-and-manufacturing (besucht am 26. 01. 2026) (siehe S. 3).

[15] *NIST Finalizes Lightweight Cryptography Standard to Protect Small Devices.* National Institute of Standards und Technology. 2025. URL: https://www.nist.gov/news-events/news/2025/08/nist-finalizes-lightweight-cryptography-standard-protect-small-devices (besucht am 26. 01. 2026) (siehe S. 3).

Hinweis zur KI-Nutzung: Bei der Erstellung dieses Artikels wurde ein KI-Sprachmodell zur Unterstützung bei Strukturierung und Formulierung eingesetzt. Die inhaltliche Verantwortung liegt bei der verfassenden Person.