Sichere Datenübertragung und **Netzüberwachung per LoRaWAN**

Seit der Einführung von Mobilfunk dreht sich die Diskussion im Kern nur um die Frage der Geschwindigkeit und damit um die Frage der Bandbreite bzw. der Datenübertragungsrate. Mittlerweile gewinnt die fünfte Generation des Mobilfunkstandards (5G) auch in Deutschland an Verbreitung, seit im Jahr 2019 die dafür notwendigen Frequenzen versteigert wurden. Der neue Standard 5G baut auf dem bestehenden Standard „Long Term Evolution" (LTE) auf und wird in einem ersten Schritt Datenraten bis 10 GBit/s ermöglichen. Derartig hohe Geschwindigkeiten lassen sich sonst nur mit Lichtwellenleiterverbindungen realisieren. Im Gegensatz zu einer leitungsgebundenen Verbindung besteht aber beim Mobilfunk die Option der gleichzeitigen Echtzeitübertragung auf weltweit 100 Mrd. Mobilfunkgeräte bei Latenzzeiten von unter einer Millisekunde bis wenigen Millisekunden.

Ermöglicht wird die hohe Datenübertragungsgeschwindigkeit durch höhere Frequenzen mit bis zu 26 GHz. Der Nachteil einer Datenübertagung mit hoher Frequenz liegt aber immer darin, dass die Reichweite des Mobilfunksignals mit steigender Frequenz sinkt und somit viele Funkmasten auf kleinem Raum nötig sind. Eine Durchdringung von dickem Mauerwerk kann problematisch werden.

Den genau umgekehrten Weg geht die Technologie, die unter dem Namen „LoRaWAN" für Furore sorgt. LoRaWAN (Long Range Wide Area Network) ist eine Art WLAN für Geräte in Städten und Kommunen mit niedriger Frequenz und dadurch bedingt hoher Reichweite, iedriger Sendeleistung und tiefer Durchdringung bis in Kellergeschosse und Brunnenstuben. Damit gehört LoRaWAN zu einer der angesagten Digitalisierungstechnologien weltweit. Die relativ einfache und preiswerte Funkinfrastruktur wird von Stadtwerken eigens aufgebaut und passt damit ideal in die lokal verankerten Strukturen eines kommunalen Infrastrukturdienstleisters, s. **Bild 1**. Zur Verbesserung der Leistung sind besonders höhere Gebäude geeignet, in Einzelfällen können die Antennen mit Hilfe einer Antennenverlängerung aufgeständert werden. Eine Kooperation mit der Katholischen Kirche zur Nutzung der Kirchtürme ist in der Diskussion. Dr. Bernhard Klocke, Geschäftsführer der Stadtwerke Haltern am See GmbH: „Mit unserem Stadtwerk sind wir Infrastrukturdienstleister für die Stadt und die Menschen, die hier leben. Deshalb passt die LoRaWAN-Technologie ideal in unser Dienstleistungsangebot."

Viele Kommunen binden bereits heute eine Vielzahl von Sensoren im Kontext der Smart City zur Steuerung der eigenen Aktivitäten ein. Beispiele sind Sensoren zur Anzeige der Parkplatzbelegung, oder Füllstandanzeiger für Abfallbehälter. Weitere Anwendungen finden sich im Bereich des Smart Home, z. B. CO_2-Sensoren und Sensoren zur Überwachung der Türen und Fenster. Auch im Bereich der Landwirtschaft kann LoRaWAN über Sensoren zur Überwachung der Bodenfeuchte oder der Temperatur in Heuballen sinnvoll eingesetzt werden (Smart Farming).

So hat LoRaWAN bereits unzählige Beispiele für die zügige Digitalisierung im Internet der Dinge ermöglicht.

Der Einsatz von klassischem WLAN oder LoRaWAN im Kontext kritischer Infrastrukturen, also in einer Umgebung mit erhöhtem Sicherheitsbedarf und/oder von gesellschaftlichem Interesse wurde lange Zeit nicht empfohlen, bzw. konnte die anerkannten Regeln der Technik sicherer Kommunikation aus Gründen bekannter Sicherheitsmängel nicht angenommen werden. Dies gilt insb. für den deutschen Markt, da im Zuge des Gesetzes zur Digitalisierung der Energiewende erstmals Anforderungen an die WAN-Kommunikation im Bereich der kommunizierenden Messsysteme konkretisiert worden sind. Damit wurde aus ingenieurstechnischer Sicht der Stand der Technik definiert und für den Energiesektor

Bild 1: LoRaWAN Antenne auf dem Dach des Umspannwerks

wurden Anforderungen festgelegt. Eines der ersten Stadtwerke, das sich Gedanken über die Ertüchtigung von LoRaWAN für KRITIS gemacht hat, ist das Stadtwerk Haltern am See. Der vorliegende Artikel gibt den Inhalt des dreijährigen Projektes wieder, das in einem maßgeschneiderten KRITIS-Produkt resultierte.

Als geeigneten Projektpartner des Vorhabens konnte sich die PHYSEC GmbH behaupten. Sie zählt zu den innovativsten Digitalisierungsunternehmen Deutschlands, ist anerkannter Experte für LPWAN und wurde für ihre „Security and Privacy by Design"-Lösungen mehrfach ausgezeichnet. Die PHYSEC erarbeitete mit HIlfe agiler Methoden innerhalb von wenigen Monaten das Sicherheitskonzept, entwickelte gemeinsam mit den Stadtwerken Haltern am See einen Demonstrator, führt gemeinsam mit dem Max Plack Institut für Cyber Security and Privacy eine Sicherheitsanalyse durch und entwickelte das ab Ende Q1/2021 verfügbare Produkt „Smart Grid Security Gateway" über die „TLS over LoRaWAN"-Technologie (Transport Layer Security).

Der erste Anwendungsfall der KRITIS-konformen LoRaWAN Konnektivität ist die Anbindung der Niederspannungsnetzinformationen aus Ortsnetzstatio-

nen und Kabelverteilerschränken. Die regulatorischen Aspekte der Sicherheitsarchitektur umfassen:

- einen besonderen Fokus auf einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für den Betrieb eines sicheren Energieversorgungsnetzes notwendig sind (aus §11 Abs. 1a EnWG),
- kryptografische WAN-Anforderungen für Messsysteme im Einsatzgebiet der Netzbetriebsmittel mit der Referenz auf die technische Richtlinie TR-03116-3 (aus IT-Sicherheitskatalog nach §11 Abs. 1a EnWG),
- angemessene technische Vorkehrungen zum Schutz des Fernmeldegeheimnisses bei der Übertragung und der Verarbeitung in Infrastrukturkomponenten (aus §109 Abs. 1 TKG),
- eine Berücksichtigung des Stands der Technik für öffentliche Telekommunikationsnetze sowohl in Maßnahmen als auch in der Sicherheitskonzeption, da im Falle LoRaWAN aufgrund der hohen Reichweite die Exklusivität und somit die Begrenzung des Teilnehmerkreises nicht erfüllt sein könnte,
- zukünftige Anforderungen im Bereich des verpflichtenden Einsatzes von Systemen zu Angriffserkennung für informationstechnische Systeme, sowie deren Einbindung in bestehende Managementsysteme und/oder in das Security Information and Event Management (aus §8 Abs. 1a IT-SiG v.2.0),
- technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zum Schutz informationstechnischer Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit maßgeblich sind (aus §8a BSIG) und alle bekannten und relevanten gesetzlichen Anforderungen.

„Innovative Technologien wie LoRaWAN so zu erweitern, dass sie mit gutem Gewissen im kritischen Infrastrukturkontext eingesetzt werden können, war 2016 noch eine wilde Idee, die 2021 serienreif wurde“ sagt Dr. Christian Zenger, Geschäftsführer der PHYSEC GmbH. Besonders relevant ist die Umsetzung des Stands der Technik für die Kommunikation über das Internet bei Messsystemen durch Erfüllung kryptografischer Anforderungen aus verwandten Bereichen. Um die Anforderungen an die WAN Kommunikation aus den referenzierten technischen Richtlinien erfüllen zu können, konnte auf „TLS over LoRaWAN“ zurückgegriffen werden. Hierbei handelt es sich um eine bereits im Vorfeld durch die Gelsenwasser AG und PHYSEC entwickelte LoRaWAN Erweiterung für funkende Wasserzähler. Die eingesetzte Security Middleware (beinhaltet Certificate Authority, Public Key Infrastructure, Key Management, TLS-Server, etc.) musste je nach LoRaWAN-Netz-Betreiber nur leicht angepasst werden. Das LoRaWAN Netz selbst, also Gateways und Netzwerk Server, bleiben unangetastet.

Neben den Werkzeugen zur Integration und zum sicheren Wirkbetrieb besteht die Lösung aus drei Komponenten:

- Nachrüstbares Messsystem mit ModBus-RTU Schnittstelle sowie
- der Beistellung des abgesicherten ModBus-zu-LoRaWAN-Konnektors.
- Der von PHYSEC für KRITIS entwickelten Datendrehscheibe und Security-Plattform IoTree.
- Die Anbindung einer Smart Grid Plattform.

Nach erfolgreicher Konzeptionierung und Softwareentwicklung wurde ein Demonstrator mit 50 Geräten für einen Feldversuch produziert. Die Technik konnte so über 20 Monate hinweg in über 30 Ortsnetzstationen und Kabelverteilern in Haltern und drei weiteren Städten erfolgreich getestet werden.

Tabelle 1: Bei guter Netzqualität können bis zu 1.480 Register alle 15 min zuverlässig übertragen werden. Bei einer schlechten Netzgüte können lediglich bis zu 40 Registerwerte zuverlässig alle 15 min übertragen werden. Letztes ist in den meisten Fällen bereits ausreichend

Spreizfaktor	Übertragungsinter-vall [Minuten]	Anzahl Register
7	15	~ 1.480
12	15	~ 40
7	60	~ 5.990
12	60	~ 200

Je nach Güte des LoRaWAN Netzes können so zwischen 40 und 1.480 ModBus-Register alle 15 min ausgelesen und übertragen werden. **Tabelle 1** zeigt diesen Zusammenhang. Bei ausreichender Netzgüte lassen sich die Register auch auf mehrere in Serie-geschaltete Messgeräte oder Intervalle verteilen. Die Konfiguration findet dabei direkt über LoRaWAN statt, sodass hier eine hohe Flexibilität ermöglicht wird. Den Ergebnissen liegt die im Feldversuch evaluierte Paketfehlerrate von ca. 20 % zugrunde (wie sie bei LoRaWAN üblich ist). Für die Berechnung wurde eine Registerbreite von 4 Byte pro Register angenommen, da in dieser Domäne häufig hochaufgelöste Fließkommazahlen verwendet werden.

Das Ergebnis des Feldversuchs motivierte und veranlasste die Entwicklung des Produkts “Smart Grid Security Bridge“. Die Serientaugliche Entwicklung inkl. LoRaWAN-Zertifizierung und unabhängiger Produktprüfung einer BSI-zertifizierten Prüfstelle wird nach Plan im Q2/2022 abgeschlossen. Die KRITIS-konforme Digitalisierungslösung auf Basis von LoRaWAN wurde für Unternehmen, Energieversorger und Kommunen entwickelt.

Autoren:
Dr. Christian Zenger und
Dr. Bernhard Klocke

Kontakt
Stadtwerke Haltern am See GmbH
Tel.: +49 2364 9240-0
info@stadtwerke-haltern.de
www.stadtwerke-haltern.de