

Das energieeffiziente RZ

Optimierte Kühlung und Klimatisierung

Stromverbrauch unter Kontrolle

Colocation legt zu

Mit Marktübersicht

Intelligente PDUs



E-Mail-Verschlüsselung mit Cryptshare
Sichere Kommunikation unter der Lupe

NarrowBand für das Internet der Dinge
Alternativen zur Breitband-Technik

Schwer
Virtu
M

Sonderdruck NewTec
NarrowBand für
das Internet
der Dinge

Industrial IoT

NarrowBand für das Internet der Dinge

Das Internet der Dinge. Unendliche Möglichkeiten. Milliarden vernetzte Geräte. Wir schreiben das Jahr 2019 und fragen uns: Auf welchem Weg sollen all die intelligenten Geräte miteinander kommunizieren? LTE? 5G? Bei genauem Hinsehen wird schnell klar: Die Breitbandtechnik ist nicht immer das Mittel der Wahl, wenn Hersteller ihre Maschinen, Ausrüstung und Produkte drahtlos miteinander verbinden wollen.

Nicht nur im Consumer-Bereich, auch in vielen Branchen wie Industrie, Hoch- und Tiefbau, Logistik, Smart City, Gebäude-Management oder der Land- und Energiewirtschaft bietet das IoT (Internet of Things) große Chancen. Dies gilt überall dort, wo Unternehmen auf prozessrelevante Daten zugreifen wollen, beispielsweise auf Produkt-, Betriebs-, Zustands-, Umgebungs- oder Ortsdaten.

Per drahtloser Vernetzung lassen sich so beispielsweise die Betriebsstunden von Leihmaschinen überwachen und ihr Standort lokalisieren. In der Logistik wird ein Echtzeit-Tracking möglich. Auch intelligente Parkleitsysteme oder eine kontinuierliche Überwachung der Batterien einer E-Mobil-Flotte gelingen per Funkvernetzung.

Voraussetzungen für ein funktionierendes Internet der Dinge

Während derzeit viel über den flächendeckenden Ausbau der Breitbandnetze und die Möglichkeiten von 5G diskutiert wird, gerät fast in Vergessenheit, dass es beim Internet der Dinge meist gar nicht um maximale

Bandbreiten und maximale Geschwindigkeiten geht. Autonomes Fahren ist zwar ohne schnelle Datenverbindungen nicht denkbar. Andererseits werden Produktions-



NTSecureNode verfügt über ein spezielles Hardware-Security-Element, das es ermöglicht, besonders sensible Daten so zu verschlüsseln, dass sie sich selbst von der Cloud nicht oder nur in anonymisierter Form lesen lassen. Diese Daten sind dann nur auf dem Endgerät des entsprechenden Benutzers lesbar.

Bild: NewTec

maschinen keine hochauflösenden Fotos verschicken und Kühlbehälter keine Echtzeit-Videodaten an Smartphones senden.

Wichtig für die Vernetzung von Geräten, Maschinen und Sensoren im Internet of Things sind vielmehr eine gute Netzabdeckung, auch innerhalb von Gebäuden, sowie eine robuste Übertragung, auch über

größere Entfernungen. Dabei schwächeln bekanntlich die herkömmlichen drahtlosen Breitband-Techniken. Eine weitere Kernanforderung ist der sparsame Umgang mit Energie. Niemand möchte jede Woche die Batterien seiner vernetzten Geräte wechseln.

Eine weitere Voraussetzung für den Erfolg des drahtlosen IoT ist der Kostenfaktor. Sowohl die Ausrüstung von Geräten und Maschinen mit Vernetzungstechnik als auch deren Betrieb im Netz sollte kostengünstig sein. Und wenn alles erfolgreich vernetzt ist, sollten die Funknetze möglichst nicht gleich unter der Last Tausender kommunizierender Geräte und Sensoren kollabieren. Eine weitere wichtige und immer noch gern unterschätzte Voraussetzung für das IoT ist eine hohe Datensicherheit.

Die eierlegende Wollmilchsau

Das „3rd Generation Partnership Project“ (3GPP), eine weltweite Kooperation zur Standardisierung der Mobilfunktechnik, veröffentlichte im Jahr 2016 eine Reihe von innovativen Funktechnik-Standards für das Low Power Wide Area Network (LPWAN). Einer dieser Standards ist Narrow-Band IoT (NB-IoT oder LTE Cat-NB1). Tatsächlich bietet diese schmalbandige Funktechnik optimale Bedingungen für die Vernetzung von Geräten, Maschinen und Sensoren.

Basis dabei ist die Konzentration auf das Wesentliche. Niedrige Datenraten von maximal 250 kBit/s im Down- und Upload ermöglichen eine Beschränkung der Träger-Bandbreite auf 200 kHz.

Die Reduktion der Bandbreite sowie niedrige Frequenzen im 800- und 900-MHz-Bereich ermöglichen eine gute Gebäudedurchdringung, da langwellige Funksignale niedrigerer Frequenz Hindernisse besser durchdringen als höherfrequente LTE-Signale. Bei schlechtem Empfang lässt sich zudem die Nachrichtenübertragung wie-

derholen, was für zusätzliche Übertragungssicherheit sorgt. Dank der niedrigen Frequenz und einer robusten Modulationstechnik können Systeme mit NB-IoT auch größere Distanzen von bis zu 30 km überwinden, sodass zuverlässige Datenverbindungen nahezu ohne geografische Einschränkungen möglich sind. Da jedes Gerät per direkter Langstreckenverbindung mit dem Server kommuniziert, sind keine zusätzlichen Peripheriegeräte oder Gateways nötig. Dies hält die Gesamtbetriebskosten gering. NB-

IoT verbraucht zudem deutlich weniger Energie als andere Funkstandards. Kleine Datenpakete, die in längeren Intervallen übertragen werden, erfordern auch nur kleine Batterien. Bei typischem Datenverkehr lassen sich so Batterielaufzeiten von bis zu zehn Jahren erreichen.

Zügiger Netzausbau

Seit der Veröffentlichung des NB-IoT-Standards in 2016 schreitet der Netzausbau in Europa und den USA schnell voran. Möglich ist dies, weil die auf LTE basierende Technik die LTE-Infrastruktur und LTE-Ressourcen wie Basisstationen, Antennen oder das lizenzierte LTE-Spektrum nutzen kann. Es muss also kein neues Netz aufgebaut, sondern nur ein bestehendes „aufgerüstet“ werden.

NarrowBand IoT ist auf diese Weise bereits in den USA und neun europäischen Ländern eingeführt. In den Niederlanden ist das schmalbandige Netz bereits seit Mitte 2017 flächendeckend verfügbar. Österreich und die Slowakei sind seit 2018 landesweit abgedeckt. Die Tschechische Republik, Polen, Ungarn, Kroatien und Griechenland planen einen landesweiten Rollout bis Ende 2019.

Für Deutschland meldete Vodafone im August 2018, NB-IoT sei in rund 90 Prozent des eigenen LTE-Netzes verfügbar. Damit schafft der Carrier nach eigenen Aussagen die Kapazität zur Vernetzung von vier Milliarden Geräten. Im Juni 2019 gab auch die



Lückenloses Kühlketten-Management in der Logistik ist kein Problem, wenn jede Lieferung mit einem NB-IoT-fähigen Sensor ausgestattet ist, der in definierten Abständen verschlüsselte Temperaturdaten an die zentrale Cloud schickt.

Bild: NewTec

Telekom bekannt, ihr NB-IoT-Netz stehe nun landesweit zur Verfügung und decke insgesamt 90 Prozent der Fläche Deutschlands ab. Damit sind die infrastrukturellen Grundlagen für die drahtlose Vernetzung einer großen Zahl von Geräten und Sensoren geschaffen.

Aber wie sieht es bei den Endgeräten aus? Wie können Hersteller ihre Maschinen, Ausrüstung und Produkte NB-IoT-fähig machen, insbesondere wenn sie über kein eigenes Know-how für die Entwicklung in diesem Bereich verfügen? Eine sichere, schnelle und kostengünstige Lösung soll der einbaufertige Sensorknoten des Security-Spezialisten NewTec darstellen. Der NTSecureNode bündelt Sensordaten, puffert und filtert sie und funkt sie schließlich in verschlüsselter Form per NarrowBand IoT zum Server oder in die Cloud. Dabei sind weder ein Gateway noch weitere Infrastruktur nötig. Der Sensorknoten verbindet sich direkt über den Netz-Provider mit der Cloud.

Dabei hat der Sensorknoten bereits alles an Bord, was zur Vernetzung via NarrowBand IoT nötig ist. Übertragungsparameter, Datenkompression, Datenauswahl und Pufferung sind über eine mobile App oder das Internet mit dem Frontend der Cloud konfigurierbar. An Bord sind außerdem Sensoren für Temperatur, Licht, Vibration, Feuchtigkeit, Druck und GPS-Lokalisation. Damit lassen sich die häufigsten Anwendungen ohne zusätzliche Hardware

umsetzen. Für spezielle Anwendungen kann der Betreiber weitere Sensoren anschließen. Die Versorgung des Boards geschieht durch einen Lithium-Akku.

Security First

Das Thema IT-Security ist im Zusammenhang mit dem Internet der Dinge immer noch unterschätzt. Gelegentlich nimmt die Öffentlichkeit mit Staunen wahr, wenn ein smarter Fernseher gehackt wird oder die Uralt-Software einer vernetzten Küchenmaschine Manipulationen von außen

Tür und Tor öffnet. Dabei ist die Datensicherheit eine Grundvoraussetzung für das Internet der Dinge.

Durch die direkte Kommunikation mit dem Internet hat Datensicherheit auch in Low-Power-Wide-Area-Netzen (LPWAN) hohe Priorität. NarrowBand IoT kann auch hier punkten, denn es stehen die im LTE-Standard implementierten Sicherheitsmechanismen zur Verfügung. Um sicherzugehen, dass das richtige Gerät mit der richtigen Cloud kommuniziert, läuft die Verifizierung beim Zugriff auf das NB-IoT-Netz sowohl für das Gerät als auch für die Cloud über sichere Schlüssel ab. Dabei kommen Verschlüsselungs-Codes von 128 bis 256 Bit zum Einsatz, mit denen die Datenübertragung per Ende-zu-Ende-Verschlüsselung vor potenziellen Angriffen geschützt ist.

Um den Verschlüsselungsvorgang so sicher wie möglich zu machen, sind die Security-Mechanismen beim NBSecure Node von NewTec bereits in der Hardware implementiert. Der Sensorknoten verfügt dazu über eine spezielle Crypto-Zelle, die verschiedene Verschlüsselungs-Algorithmen unterstützt. Auch sichere Firmware-Updates „over the air“ sind so möglich. Über die Absicherung der Luftschnittstelle hinaus ist es aber auch wichtig, die Nutzdaten komplett Ende zu Ende zu verschlüsseln. NTSecureNode verfügt zu diesem Zweck über ein spezielles Hardware-Security-Element, das es ermöglicht, besonders

sensible Daten so zu verschlüsseln, dass sie sich selbst von der Cloud nicht oder nur in anonymisierter Form lesen lassen. Diese Daten sind dann nur auf dem Endgerät des entsprechenden Benutzers lesbar. Ein weiterer sensibler Punkt ist die Authentifizierung zwischen Cloud und Knoten, die sich durch das Security-Element ebenfalls wesentlich sicherer und einfacher gestaltet. Im Zusammenspiel mit einer sicheren Cloud wie NewTecs NTSecureCloud bildet der Sensorknoten so einen abgeschlossenen, kryptographischen Raum. Hohe Daten- und Prozesssicherheit stehen so als Plug-and-Run-Lösung für viele Anwendungsszenarien zur Verfügung. In der näheren Zukunft wird wohl kaum eine Branche ohne Vernetzung ihrer Maschinen, Ausrüstung oder Produkte auskommen. Besonders dort, wo keine direkte Stromversorgung und keine kabelgebundene Technik zur Verfügung stehen, spielt NB-IoT seine Stärken aus. Ein Beispiel ist das Gebäude-Management. Daten zum Wärmeverbrauch können direkt am Heizkörper gesammelt und zentral in einer Cloud zur Auswertung abgelegt werden –

NBSecure Node hat dazu einen Wärmesensor an Bord. Auch Erdgas oder Wasserzähler ohne eigenen Stromanschluss im Keller lassen sich über NB-IoT auslesen. Die Übertragung der Daten kann dann zuverlässig auch durch dicke Mauern und sogar durch die Erde geschehen. In der Smart City melden mit Sensoren ausgestattete Parkplätze an eine App, wo der nächste freie Parkplatz ist. NarrowBand IoT kann auch das Management von Leihgeräten in Landwirtschaft oder beim Bau deutlich erleichtern, indem stets aktuelle Daten über Nutzung und Einsatzort zur Verfügung stehen. Auch das Flotten-Management von E-Mobil-Flotten kann sich NB-IoT zunutze machen: Anhand aktueller Daten zum Ladezustand und technischen Zustand der Batterien können Betreiber etwa die Lade- oder Wartungsvorgänge von E-Gabelstaplern zuverlässig zentral planen. Lückenloses Kühlketten-Management in der Logistik ist kein Problem, wenn jede Lieferung mit einem NB-IoT-fähigen Sensor ausgestattet ist, der in definierten Abständen verschlüsselte Temperaturdaten an die zentrale Cloud schickt. Ebenso können

zerbrechliche oder druckempfindliche Waren durch Druck- oder Gyrosensoren während des kompletten Lieferwegs verfolgt werden – auch über Ländergrenzen hinweg. Europaweites NB-IoT-Roaming befindet sich zurzeit im Ausbau. Aktuell unterstützt etwa die Telekom mit ihren Töchtern in Deutschland, Österreich, den Niederlanden, Ungarn, der Slowakei und der Tschechischen Republik das grenzüberschreitende Tracking. Auch Herstellern von Consumer-Produkten bietet NB-IoT zahlreiche Möglichkeiten, ihre Produkte für die Endverbraucher aufzuwerten. So kann man zum Beispiel Fahrraddieben das Handwerk deutlich erschweren, wenn ein am Drahtesel verbauter Sensor GPS-Daten über das NB-IoT-Netz sendet. Sogar Tierbesitzer können von der Technik profitieren. Von Pet-Trackern gesendete Positionsdaten können nämlich sicherstellen, dass die geliebten vier Pfoten nie wieder tage- oder wochenlang unbekannt verreisen. Achim Brunner/jos

Achim Brunner ist Entwicklungsleiter Product Engineering bei NewTec, www.newtec.de.

News

Discovery 5.0 erhält neue Funktionen

JDisc: Automatische Netzwerk-Inventarisierung und Performance-Überwachung

JDisc hat seine Lösung Discovery um das „Measurement Add-on“ erweitert. Startet ein IT-Administrator Discovery, inventarisiert es ohne das manuelle Ausrollen von Agenten das Netzwerk, so der Hersteller.

Dabei erkenne es alle gängigen Betriebssysteme wie Windows, Linux, VMware, MAC OS X, HP-UX, AIX, Solaris oder FreeBSD. Darüber hinaus soll Discovery Router, Switches, Drucker und viele andere Gerätype-

pen identifizieren können. Bis zu 2.000 Geräte wertet Discovery nach Bekunden des Herstellers pro Stunde aus.

Die neue Version 5.0 erweitert mit dem „Measurement Add-on“ den Funktionsumfang der Lösung weiter. Zusätzlich zu den eher statischen Inventardaten ermittle das Add-on Daten zur Auslastung. Auf Windows hat das Add-on laut JDisc über selbst definierbare Templates Zugriff auf alle Windows-Performance-Monitor-Daten. Bei anderen Geräten wie beispielsweise Drucker, Router und Switches erhebe es die Auslas-

tungsdaten über SNMP. Zu den weiteren Verbesserungen, die JDisc mit Version 5 einführt, gehört etwa die leichtere Erkennung von Computern, die nur unregelmäßig mit dem Netzwerk verbunden sind. Sie sollen sich mit dem neuen „Directory Logon Scanning“ ohne Veränderungen oder Verteilung von Login-Skripten zeitnah erfassen lassen.

Auch die Erkennung von Docker-Containern hat der Hersteller nach eigenen Bekunden verbessert. ts

Info: JDisc
Web: www.jdisc.com



JDisc bietet auch eine kostenlose Starter Edition der Lösung an. Bild: JDisc