22. Nachwuchswissenschaftler*innenkonferenz (NWK)

https://doi.org/10.52825/ocp.v2i.146

Publiziert: 15. Dez. 2022

Einsatz von Funktechnologien im Industrieumfeld mit Blockchain

Vinzenz Lorenz[1*]

[1] Hochschule Mittweida

[*] Korrespondenz: lorenz1@hs-mittweida.de

Kurzfassung. In dem Beitrag wird die Entwicklung eines OpenThread-Netzwerks im Rahmen eines BMBF-Projekts vorgestellt, mit dem Produktionsdaten in eine private Blockchain übergeben werden sollen, um die Daten fälschungssicher und transparent zu speichern. Dafür wurden u. a. spezielle Funkmodule entwickelt, welche die Funkstandards OpenThread und Bluetooth Low Energy unterstützen und somit zusätzlich die Anbindung mobiler Endgeräte an die private Blockchain ermöglichen. Bei der Konzeption und Entwicklung der Funkmodule sowie der Kommunikationsprotokolle wurde darauf Wert gelegt, dass das Funknetz den hohen Anforderungen an seinen Einsatz im Industrieumfeld, wie Inbetriebnahme durch Plug-&-Play, Robustheit, Verfügbarkeit, Datendurchsatz, Latenz und vor allem IT-Sicherheit, gerecht wird.

1. Einleitung

Die grundlegenden Schutzziele für die Kommunikationstechnik sind Vertraulichkeit, Integrität und Verfügbarkeit. Diese finden in unterschiedlicher Art Anwendung. Eine permissioned Blockchain erbringt diese Schutzziele und liefert zusätzlich die Verbindlichkeit der Daten [1]. Diese Vorteile können auch in drahtlosen Netzwerken eingesetzt werden. Über die Anbindung von diesen Netzwerken an eine Blockchain können Produktionsdaten fälschungssicher und transparent hinterlegt werden [2; 3; 4]. Im Rahmen des safe-UR-Chain Projektes, gefördert durch das BMBF [5], wurde ein drahtloses Netzwerk entwickelt, das diese Aufgaben erfüllt. Diese sind im industriellen Einsatz mit hohen Anforderungen verbunden: Inbetriebnahme durch Plug-&-Play, Robustheit, Verfügbarkeit, Datendurchsatz, Latenz und vor allem IT-Sicherheit [6; 7].

Die Anbindung des Funknetzwerkes erfolgt über s. g. Thin-Nodes, die keine vollständige Kopie der Blockchain besitzen. Sie geben die Transaktionen an die Full-Nodes weiter, die diese Transaktionen ausführen und in das Netzwerk bringen [1]. Die Thin-Nodes haben eine direkte Verbindung mit der Infrastruktur der Produktionsumgebung, wodurch Prozessdaten, Statusmeldungen und Warnungen direkt in die Blockchain gelangen. Die Funkkommunikation mit der Anbindung mobiler Geräte bildet hierbei die Schnittstelle zum Nutzer. Die Kommunikation soll durch selbst entwickelte Funkmodule erreicht werden, die in die Thin-Nodes integriert werden.

Das Funknetzwerk mit mobilen Geräten soll dabei den Produktionsmitarbeiter in der Wartung und dem Management des Fertigungsprozesses unterstützen und Statusinformationen aus der Blockchain übermitteln. Ein weiterer Anwendungsfall ist die Freigabe von Meisterstücken an Fertigungsanlagen, die durch einen Mitarbeiter geprüft werden. Die Bestätigung gelangt durch mobile Geräte in die Blockchain und erhöht die Transparenz in der Produktionsumgebung. Der Abruf von Maschineninformationen von der Blockchain über mobile Endgeräte erleichtert die Mensch-Maschine-Kommunikation.

2. Methoden

Es sind verschiedene Methoden in diesem Projekt zum Einsatz gekommen. Eine davon war, den Ist-Stand der Übermittlung der Produktionsdaten sowie deren Verlauf und deren Manipulation zu ermitteln. In Zusammenarbeit mit den Industriepartnern des Konsortiums konnten somit tiefe Einblicke in die Abfolge von Produktionsabläufen und die Sicherheit der anfallenden Daten gewonnen werden. Dabei zeigte die Analyse, dass bereits ein hoher Sicherheitsstand vorhanden ist und nur geringe Ansatzpunkte existieren, die eine Manipulation der Daten ermöglichen. Verbesserungsbedarf wurde in der Verbindlichkeit und Transparenz der Daten gesehen. Die Nachverfolgung, welcher Nutzer welche Daten verändert, in Produktionsprozesse eingreift oder auch Statusmeldungen ignoriert und bestimmte Prozesse genehmigt, ließ hier durch den Einsatz einer Blockchain neue Anwendungsmöglichkeiten zu.

In der hardwarenahen Softwareentwicklung der Funkmodule kam vor allem das V-Modell zum Einsatz. Das V-Modell sieht iterative Schritte vor und beinhaltet entwicklungsbegleitende Tests. Diese Tests und Erprobungen hatten einen großen Einfluss auf die Softwareentwicklung. Die Entwicklungsstrategie glich daher einer experimentellen Entwicklung, wobei Entwicklungsansätze verfolgt wurden und die dazugehörigen Tests den weiteren Entwicklungsweg bestimmten.

3. Konzeption

3.1 OpenThread und Bluetooth Low Energy

Die Funkmodule sollen zeitgleich zwei Funkübertragungstechnologien unterstützen. Auf der einen Seite sollen sie ein OpenThread-basiertes Mesh-Netzwerk aufbauen [8], das die Thin-Nodes des Blockchain-Netzwerks drahtlos miteinander verbindet. Auf der anderen Seite sollen sie die drahtlose Kommunikation der Thin-Nodes mit den mobilen Endgeräten über Bluetooth Low Energy (BLE) ermöglichen [9]. Hierfür ist ein Stack notwendig, der beide Technologien zeitgleich unterstützt. Dieser Stack wird von Nordic Semiconductor angeboten, und zwar auf dem Chip nRF52840 [10]. Eine gleichzeitige Unterstützung beider Technologien hat den Vorteil, dass die Funkprotokolle in ihrem vorgesehenen Zeitschlitz arbeiten und das Senden und Empfangen von Daten von keinem der verwendeten Funkprotokolle unterbrochen wird. Gearbeitet wird hier mit einem Zeitmultiplex [11], wie es die Abbildung 1 darstellt.

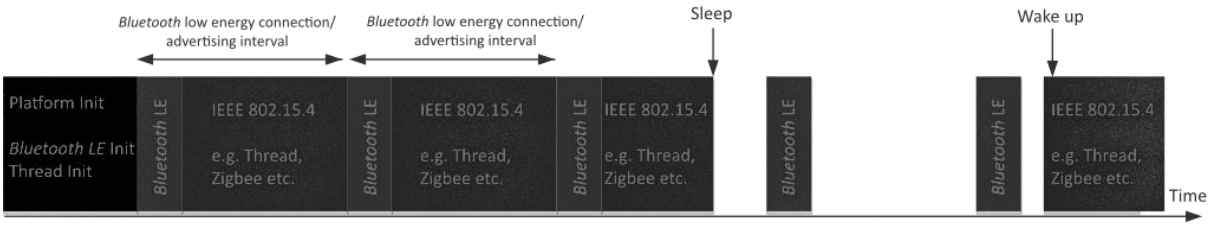

Abbildung 1: Zeitmultiplex, [11]

Das Advertising- und Connection-Intervall von BLE legt die Intervalldauer für das Zeitmultiplex fest, in dem der Wechsel zwischen den Funkprotokollen stattfindet. Um die Latenz von Thread und BLE gering zu halten, wurde in diesem Projekt mit einem Connection-Intervall von 100-200 ms gearbeitet. Der Datendurchsatz beträgt bei der BLE-Duplex-Verbindung je Richtung 390 kbit/s [12]. Die Datenrate von Thread ist um ein Vielfaches geringer als von BLE. Mit ca. 45 kbit/s ist eine Übertragung großer Datenmengen nicht möglich [8].

3.2 Allgemeiner Aufbau und Architektur

Die Abbildung 2 zeigt die Architektur des Gesamtsystems. Jeder Thin-Node ist mit einem Funkmodul ausgerüstet und kann über OpenThread und BLE Daten austauschen. Die Kommunikation mit dem Blockchainnetzwerk und einem mobilen Endgerät ist nur über BLE möglich. Alle Thin-Nodes sind Zugangspunkte für die mobilen Geräte und ermöglichen dem Nutzer Zugriff auf die Blockchain. Die Schnittstelle zwischen dem Funkmodul und dem Thin-Node wurde über ein UART-Interface realisiert. Sie übermittelt Anfragen und Daten in die Blockchain. Neben den Thin-Nodes, die jeweils über ein Funkmodul verfügen, gibt es auch Funkmodule, die im Standalone-Betrieb arbeiten und keine Verbindung zur Blockchain haben. Diese Module erweitern die Reichweite des Funknetzes und bilden zusätzliche Zugangspunkte für mobile Geräte. Im Hintergrund arbeitet der OpenThread-Funkstandard, der alle Funkmodule miteinander verbindet und eine bidirektionale Kommunikation zwischen den mobilen Geräten und den Thin-Nodes sicherstellt.

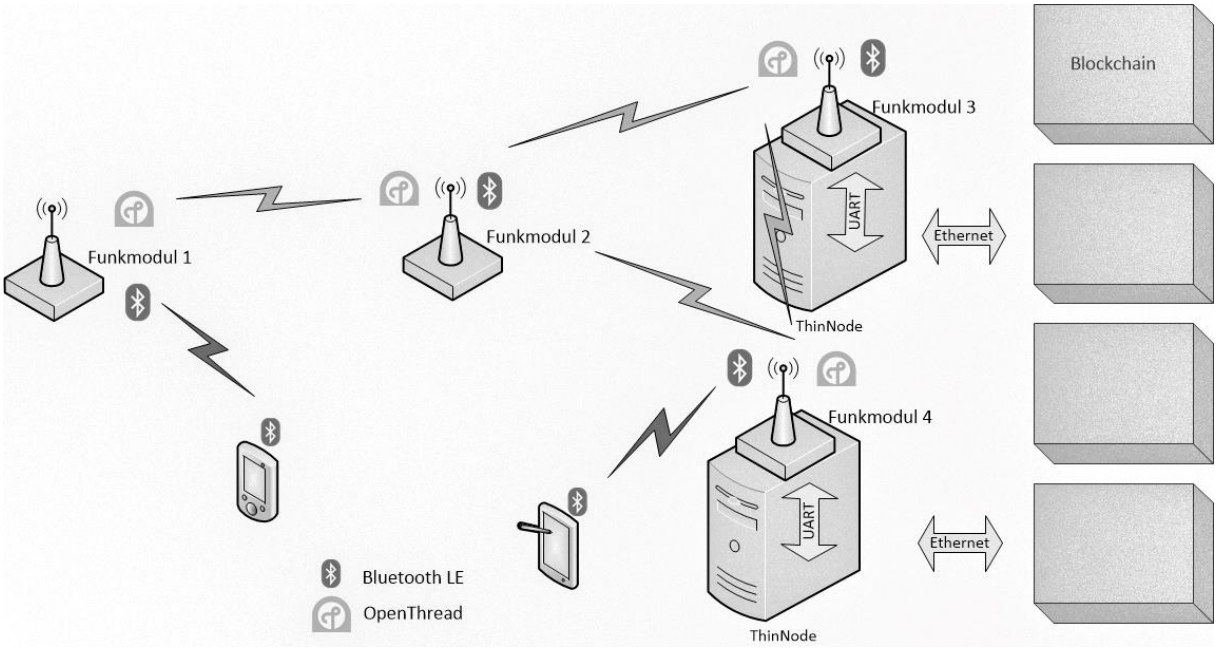

Abbildung 2: Architektur des Gesamtsystems, [eigene Darstellung]

3.3 Protokollentwicklung

Es wird deutlich, dass eine Vereinigung von OpenThread, BLE und UART über ein zusätzliches Protokoll erfolgen muss, um die Datenübertragung zwischen den Funkkomponenten und der Blockchain zu garantieren. Die Aufgabe des Protokolls ist es, die verschiedenen Adressen von BLE und OpenThread verfügbar zu machen, um eine übergeordnete Übertragung über mehrere Funkstandards zu gewährleisten.

Teil des übergeordneten Protokolls sind eigene Framestrukturen und Kommunikationsabläufe, die auf die Besonderheiten der Funkprotokolle angepasst sind. Dazu gehört, die verschiedenen Adressen von OpenThread und BLE zu unterscheiden und ineinander zu übersetzen. OpenThread arbeitet mit einer 16 Byte großen Mesh Local ID (MLEID), die jedes Gerät eindeutig identifiziert und auch bei erneuten Anmeldevorgängen und Verbindungsänderungen bestehen bleibt. Sie eignet sich damit sehr gut für die Adressierung der einzelnen Funkmodule im Thread-Netzwerk. Die Übertragung der Daten zum Zielknoten erfolgt selbstständig durch die Nutzung valider Routen. BLE arbeitet mit einer 6 Byte MAC-Adresse, die für die Adressierung in einem Netzwerk nutzbar ist.

Jedes Funkmodul hat eine eigene Registrierungstabelle (RegTable), in der die MLEID-Adressen der Funkmodule im OpenThread-Netzwerk und die BLE-Adressen der mobilen Geräte zugeordnet sind. Bei der Anmeldung eines neuen mobilen Gerätes sendet dieses über die verschlüsselte OpenThread-Verbindung die Zuordnung an alle Teilnehmer im Netzwerk.

3.4 Analyse der Sicherheitsniveaus von OpenThread und BLE

Die Sicherheit der drahtlosen Kommunikation steht in diesem Projekt an erster Stelle und kann auf die höchsten IT-Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit fokussiert werden. Das OpenThread-Netzwerk erfüllt diese IT-Sicherheitsziele durch den Einsatz von Advanced Encryption Standard - Counter with Cipher Block Chaining Message Authentication (AES-CCM). Das CCM-Verfahren ermöglicht die simultane Verschlüsselung und Authentifizierung der Daten vor ihrer Übertragung. Gesichert ist die Verbindung mit einem 128 Bit Masterkey, der in der Cryptocell des nRF52840 abgelegt ist [8].

Das Bluetooth Low Energy Protokoll 4.2 ist vollständig abwärtskompatibel zu früheren BLE-Versionen, die das LE Legacy Pairing nutzen. Das neue Verfahren, das ab Version 4.2 hinzukam, ist LE Secure (LESC). Dieses Verfahren nutzt einen einzelnen 128 Bit Long Term Key (LTK), um die Verbindung zu verschlüsseln. Dieser LTK wird mithilfe des Protokolls Public-Key-Cryptography Elliptic Curve Diffie Hellman (ECDH) ausgetauscht, das im Vergleich zum ursprünglichen BLE-Schlüsselaustauschprotokoll eine deutlich höhere Sicherheit bietet. Zusätzlich verfügt BLE über verschiedene Sicherheitslevel, um allen Anforderungen gerecht zu werden. Von Level 0 ohne Zugriffseinschränkungen bis Level 4 höchste Sicherheit. In Level 4, das in diesem Projekt Anwendung findet, nutzt BLE das LESC-Verfahren. Den notwendigen Schutz vor MITM-Attacken bietet eine sichere Pairing-Methode. In diesem Projekt wird mit Out of Band (OOB) Pairing und dem Passkey-Verfahren gearbeitet [9].

3.5. Erhöhung der Sicherheit durch die Symbiose aus OpenThread und BLE

Bei der Nutzung von BLE mit LESC und Level 4 ergeben sich einige Nachteile für den Nutzer. So ist es notwendig, bei einem Wechsel eines BLE-Zugangspunktes ein erneutes Pairing mit dem Funkmodul durchzuführen. Das ist in der Praxis nur schwer zu realisieren, denn bei jedem neuen Anmeldevorgang an einem neuen Funkmodul müsste eine Passkey-Eingabe oder ein NFC-Datenaustausch erfolgen. Gelöst wurde das Problem durch die Entwicklung eines eigenen Verfahrens, das durch das OpenThread-Netzwerk den Schlüsselaustausch im Hintergrund für die mobilen Geräte organisiert. Die Abbildung 3 zeigt ein mögliches Szenario. Der Nutzer meldet sich einmalig bei dem Funkmodul 1 über NFC an und verbindet sich damit über BLE (Schritt 1). Im Hintergrund sucht das mobile Gerät Funkmodul 2 und initiiert auch hier einen Verbindungsaufbau (Schritt 2). In diesem Fall wird das Passkey-Verfahren genutzt. Der Passkey wird über OpenThread an Funkmodul 1 geschickt, worüber das mobile Gerät den Passkey erhält (Schritt 3). Jede weitere Verbindung zu anderen Funkmodulen kann mit dem gleichen Verfahren durchgeführt werden.

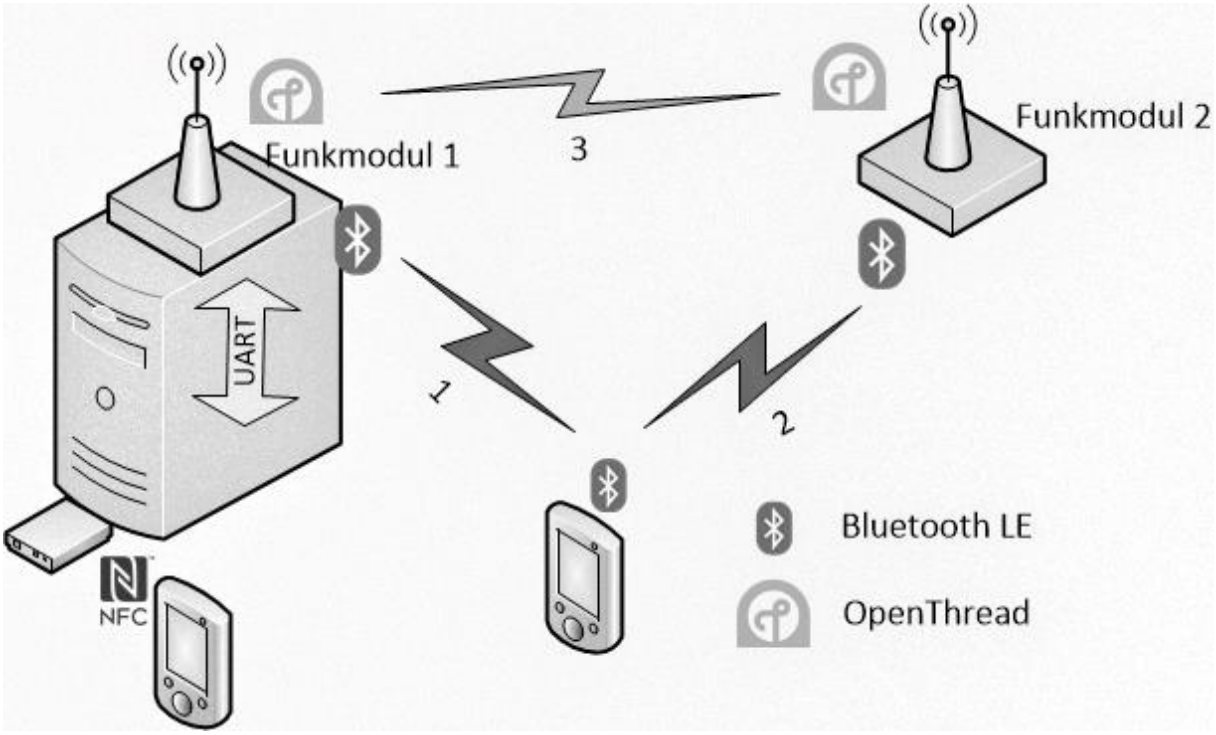

Abbildung 3: Übertragung des Passkeys beim Pairing,
[eigene Darstellung]

Abbildung 4: entwickeltes Funkmodul, [eigenes Foto]

4. Hardwareentwicklung

Als Thin-Node wurde ein Hilscher NetPi ausgewählt. Dieser Industrie-PC bietet eine Schnittstelle für eigene Hardwareentwicklungen und schützt mit seinem Metallgehäuse gut gegen EMV-Störungen.

Das entwickelte Thin-Node-Funkmodul ist in der Abbildung 4 dargestellt. Für das Design des Funkmoduls war ein vierlagiges Layout notwendig, um alle erforderlichen Komponenten, wie den Chip nRF52840 mit Multiprotokollunterstützung [10], einen zusätzlichen Flash-Speicher, eine UART-Schnittstelle, die Antennen-Verbindung sowie ein Near Field Communication Interface (NFC), zu integrieren. Herausfordernd war, diese Komponenten auf einer Leiterplattenfläche von 40x40 mm zu implementieren. Ein Schwerpunkt lag auf der Anpassung und dem Tuning der Antenne. Die Antenne ist extern ausgeführt und wurde mit einem Netzwerkanalysator an die richtige Impedanz angepasst. Damit werden Reflexionen verhindert, die zu einem Leistungsabfall an der Antenne führen und die Reichweite reduzieren.

5. Softwareentwicklung

Die Umsetzung des Konzeptes aus Kapitel 3.3 erfordert die Nutzung vieler verschiedener Technologien und Protokolle. Hierfür wurde das Software Development Kit von Nordic benutzt, das den BLE-Stack und den OpenThread-Stack als Multiprotokoll in einer Entwicklungsumgebung vereint. Leider bietet Nordic keine Ready-to-Use-Lösung an, die eine zeitgleiche Nutzung der Crypto-Bibliothek für die IT-Sicherheitsverfahren von BLE und OpenThread ermöglicht. Deshalb wurde eine eigene Crypto-Bibliothek implementiert. Für den Pairing-Vorgang ist auch die Implementierung einer NFC-Bibliothek notwendig gewesen. Für die Kommunikation mit der Blockchain wurde eine UART-Bibliothek genutzt. Schwerpunkt der Softwareentwicklung war die Umsetzung des eigenen Protokolls, das auf den BLE- und OpenThread-Standard aufbaut. Dies beinhaltet u. a. die Umsetzung der konzipierten Framestrukturen und Kommunikationsabläufe sowie die Einrichtung spezieller Datenpuffer.

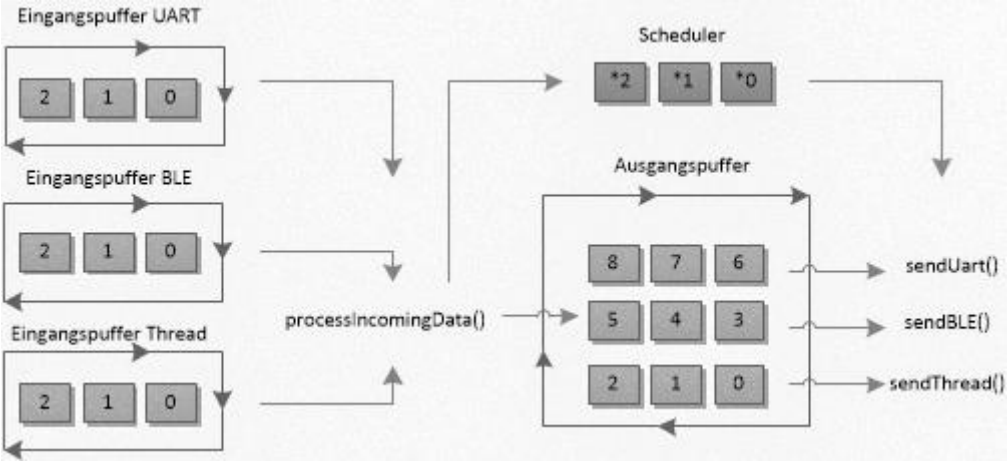

Abbildung 5: Datenpuffer, [eigene Darstellung]

Es gibt drei Eingangspuffer, die jeweils Daten erhalten (siehe Abbildung 5). Eine Thread-sichere Funktion sortiert die Daten und entscheidet, welche Daten an welchen Adressaten versendet werden. Der Scheduler legt die Sendereihenfolge fest, wofür mit Zeigern gearbeitet wird. Schlussendlich werden die Daten aus dem Ausgangspuffer durch den Scheduler versendet.

Im Rahmen dieses Projektes wurde auch eine Android-App entwickelt, die den automatischen Verbindungsaufbau mit den Funkmodulen durchführt. Außerdem musste das Kommunikationsprotokoll auch in der App implementiert werden, um einen reibungslosen Kommunikationsablauf zu den Funkmodulen und damit in die Blockchain zu gewährleisten.

6. Ergebnis/Diskussion

In diesem Projekt ist ein drahtloses Netzwerk entstanden, das die Übermittlung von industriellen Prozessdaten und Statusinformationen von mobilen Endgeräten in eine private Blockchain ermöglicht. Von den mobilen Endgeräten gelangen Quittierungen von Statusinformationen und Warnungen in die Blockchain, wodurch manipulationssicher nachvollzogen werden kann, wer zu welchem Zeitpunkt bestimmte Prozesse genehmigt und quittiert hat.

Eine weitere Innovation ist der Einsatz von mehreren Funkprotokollen auf einem Chip. Aus der gleichzeitigen Nutzung von OpenThread und BLE ergeben sich symbiotische Vorteile. OpenThread bietet eine hervorragende Möglichkeit, Mesh-Netzwerke zu bilden und ermöglicht mit dem schlüssellosen Austausch, das Netzwerk in Plug-&-Play aufzubauen. Durch die Vernetzung der einzelnen Funkmodule kann das Netzwerk zudem beliebig erweitert werden, und zwar ohne eine Anbindung an ein drahtgebundenes Netzwerk. OpenThread basiert auf dem

Standard IEEE 802.15.4, der von den meisten mobilen Geräten nicht unterstützt wird. Dieser Nachteil kann mit dem BLE-Standard kompensiert werden. Da BLE von allen mobilen Geräten unterstützt wird, ist eine breite Anwendung möglich. Ein weiterer Vorteil der Nutzung beider Funktechnologien ist, dass der Anmeldevorgang durch den automatischen Passkey-Austausch für den Nutzer vereinfacht werden konnte. Die Vereinfachung sicherheitsrelevanter Vorgänge führt zu einer erhöhten Nutzerakzeptanz und damit auch zu einer erhöhten Sicherheit.

Datenverfügbarkeit

Der Beitrag basiert nicht auf Daten, die in irgendeiner Form veröffentlicht werden könnten.

Interessenskonflikte

Der Autor erklärt, dass keine Interessenskonflikte vorliegen.

Literaturverzeichnis

1. Erik Neumann, Kilian Armin Nölscher, Gordon Lemme, Adrian Singer, Security and traceability in civil production and value networks through blockchain, 6th International Conference on Cyber-Technologies and Cyber-Systems, 3-10. October 2021.
2. Marc Jayson Baucas and Petros Spachos, Permissioned Blockchain-Driven Internet of Things Gateway Using Bluetooth Low Energy, ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 7-11. June 2020.
3. Rishabh Jain, Prachi Malik, Deepanshu Jain, Ronak Bhatia, Pratham Taneja, File Tracking and Security System Using BLE and Blockchain, 2021 Asian Conference on Innovation in Technology (ASIANCON), 28-29. August 2021.
4. Umesh Bodkhe, Sudeep Tanwar, Karan Parekh, Pimal Khanpara, Sudhanshu Tyagi, Neeraj Kumar, Mamoun Alazab, Blockchain for Industry 4.0: A Comprehensive Review, in IEEE Access, Volume 8, 17. April 2020.
5. Bundesministerium für Bildung und Forschung, Verbundprojekt: Sicherheit und Nachverfolgbarkeit in zivilen Produktions- und Wertschöpfungsnetzwerken durch Blockchain (safe-UR-chain) - Teilvorhaben Blockchainnetzwerke mit Funkclients für kritische Infrastrukturen, Förderkennzeichen:13N15150, 27. August 2019.
6. Vaibhav Pratap Singh, Tulasi Dwarakanath V, Haribabu P, N Sarat Chandra Babu, IoT Standardization Efforts - An Analysis, 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), 17-19. August 2017.
7. Malvin Nkomo, Gerhard P. Hancke, Adnan M. Abu-Mahfouz, Saurabh Sinha and Adeiza. J. Onumanyi, Overlay Virtualized Wireless Sensor Networks for Application in Industrial Internet of Things: A Review, Sensors 2018, 18. October 2018.
8. OpenThread Group, openthread.io, [Online]. available: https://openthread.io/guides/thread-primer, 14. Februar 2022.
9. Bluetooth SIG INC, Specification of the Bluetooth System, v4.2, 2014. Nordic Semiconductor, infocenter.nordicsemi.com, [Online]. available:
10. https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsdk_tz_v4.1.0%2Fthread_ot_stack_overview.html&cp=8_3_2_0, 14. Februar 2022.
11. [Nordic Semiconductor, infocenter.nordicsemi.com, [Online]. available: https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsdk_tz_v4.2.0%2Fble_154_multiprotocol.html&anchor=ble_154_multiprotocol_dynamic, 02. Mai 2022.
12. Nordic Semiconductor, infocenter.nordicsemi.com, [Online]. available: https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_data_throughput%2Fble_data_throughput.html, 02. Mai 2022.