Kommunikationsarchitektur für das Smart Forestry-System

Inhalt

1 Einführung

Das vorliegende Whitepaper gibt einen Überblick über relevante Aspekte der Kommunikationsarchitektur des Smart Forestry-Systems zur intelligenten und clusterübergreifend integrierten Holzernte. Das Whitepaper fasst u.a. folgende Aspekte zusammen:

- Grundlegende Kommunikationstechnologien im heutigen Wald und Holz-Sektor,
- praktische Anwendungsbeispiele dieser Kommunikationstechnologien und
- die daraus abgeleitete Kommunikationsarchitektur für das Smart Forestry-System.

Diese Architektur wird zur Umsetzung der Anwendungsszenarien zur intelligenten und clusterübergreifend integrierten hochmechanisierten und motormanuellen Holzernte sowie dem Holztransport im Rahmen von Smart Forestry genutzt.

2 Grundlegende Kommunikationstechnologien

2.1 Drahtlose Übertragungstechnologien

Drahtlose Übertragungstechnologien sind eine der wichtigsten Bausteine zur Kommunikation im Wald und Holz (WH)-Sektor sowie zur Vernetzung in einem Internet der Dinge (Internet of Things, IoT). Sie stellen die Grundlage für die Vernetzung bereit. Die Art der Informationsübertragung als Teil der IoT-Kommunikation ist stark abhängig von Geräten, Nutzern und Funktionen im IoT. Daher müssen beim Design und bei der Nutzung in diesem Sektor diverse Anwendungsszenario-spezifische Aspekte berücksichtigt werden, z.B. wie stark das Netzwerk durch den Nachrichtaustausch von Kommunikationsteilnehmern ausgelastet werden kann, wie groß die Distanz zwischen ihnen sein kann etc. Somit ergibt sich ein Spannungsfeld aus

- Reichweite,
- Datendurchsatz,
- Energieverbrauch und
- Latenz.

Diese Faktoren haben einen unmittelbaren Einfluss aufeinander. Beispielsweise verbrauchen Netzwerke, über die große Datenmenge ausgetauscht werden können, im Verhältnis mehr Energie als solche für kleine Datenströme. Kommunikationstechnologien, mit denen große Entfernungen bei der Kommunikation überwunden werden können, führen in der Regel zu einer deutlich höheren Latenz.

In diesem Abschnitt werden klassische Übertragungstechnologien vorgestellt, deren Einsatz im WH-Sektor denkbar ist oder die bereits im WH-Sektor eingesetzt worden sind.

2.1.1 LTE, 4G und 5G

Long Term Evolution (LTE) wurde im Jahr 2010 als Teil der dritten Mobilfunkgeneration eingeführt (auch 3,9G genannt). Der Standard basiert auf herkömmlicher GSM- und UMTS-Netztechnologie und nutzt Modulationstechniken zur Erhöhung der Netzkapazität und -geschwindigkeit. Weiterhin nutzt LTE, im Gegensatz zu UMTS, verschiedene Kanalbandbreiten (von 1 bis 20 MHz). In Kombination mit MIMO („Multiple Input Multiple Output“, vereinfacht „Mehrantennen-Fähigkeit“) wird die Latenz im Idealfall auf 5 ms reduziert. In der aktuellen Version von LTE beträgt die theoretische Maximalgeschwindigkeit 300 Mbit/s im Download und 75 Mbit/s im Upload.

Die Bezeichnungen 4G und LTE werden von vielen Mobilfunkanbietern häufig synonym genutzt. 4G steht für die vierte Generation des Mobilfunkstandards, die auf 3G folgt und 5G vorausgeht, und erhielt

die Bezeichnung LTE+. Diese nutzt eine spektrale Bandbreite von 20-100 MHz und bietet eine theoretische Maxgeschwindigkeit von 1.000 Mbit/s im Download und 500 Mbit/s im Upload.

Seit 2019 wurde angefangen, 5G weltweit umzusetzen. Prognosen zufolge werden im Jahr 2025 mehr als 1,7 Milliarden Nutzer erwartet. 5G bietet eine Maximalgeschwindigkeit von 10 Gbit/s im Download mit einer höheren Bandbreite und einer niedrigen Latenz von 1 ms. 5G soll die Qualität der Mobilfunknetze in vielen Gebieten verbessern und auch neue Anwendungen im Bereich IoT ermöglichen, die eine hohe Anforderung an die Echtzeit-Fähigkeit verlangen. Da 5G im Normalfall in höheren Wellenlängenbereichen funkt, muss hier mit Einbußen bei der Reichweite im Vergleich zu 4G gerechnet werden, insbesondere dann, wenn Hindernisse wie Bäume eine Sichtverbindung ausschließen. Es ist jedoch zu beachten, dass 5G in bestimmten Fällen auch auf niedrigeren Frequenzen als 4G übertragen werden kann, was zu einer größeren Reichweite führt. Insgesamt hängt die Reichweite von 5G also stark von den Umgebungsbedingungen und der Art der verwendeten Ausrüstung ab.

Ein weiterer wichtiger Aspekt bezieht sich auf die Verfügbarkeit von 5G-Netzen in Deutschland. Diese lässt sich aktuell beziffern und der Ausbau dürfte in 1-2 Jahren nahezu abgeschlossen sein. Laut einer Schätzung[1] ergibt sich die folgende Übersicht der drei Mobilfunkanbieter im Jahr 2024 in Tabelle 1.

Tabelle 1: Geschätzter Stand der 5G-Netzabdeckung in Deutschland 2024

Anbieter	Ausbaustatus	Städte (ca.)	Reichweite in Mio. Bürger (ca.)
Telekom	97%	nicht verfügbar	79
Vodafone	92%	200	75
O2	96%	200	79

2.1.2 Low Power Short Range-Netzwerke (LPSRN)

Short Range-Netzwerke werden an mancher Stelle auch als “the last 100 meters”[2] in einem IoT bezeichnet. Dieser Bereich zeichnet sich dadurch aus, dass die Wege zur Vernetzung vielfältig und daher diverse konkurrierende Technologien verfügbar sind. Klassische Anwendungsszenarien dieser Netzwerke sind Smart Home und Smart Office.

Auch im Wald gibt es entsprechende Anwendungen. Praktische Beispiele sind:

- Ein Harvester steht auf einer Rückegasse und will deren Befahrbarkeit feststellen. Dafür braucht die Maschine die Bodenfeuchte von verschiedenen Bodenfeuchtsensoren. Der Harvester hat in diesem Moment keinen Internetzugang, ist aber nicht weit von den Sensoren entfernt.
- Ein Waldarbeiter will über sein Handy die Produktionsdaten des Harvesters abrufen. Da es keinen Mobilfunkempfang auf seinem Handy gibt, kann die Kommunikation nur über ein lokales LPSRN erfolgen.

2.1.2.1 Bluetooth

Bluetooth ist eine auf Ultrahochfrequenz (UHF)-Funktechnik basierende Kommunikationstechnologie, die sich für den Datenaustausch zwischen Geräten eignet, die sich nicht weit voneinander entfernt befinden. Diese Technologie ist durch einen geringen Energieverbrauch und eine Hochgeschwindigkeitsdatenübertragung geprägt und kann dazu eine Vielzahl von Daten transportieren, z.B. Sprach- und Bildsignale. Zudem kann Bluetooth zur Realisierung verschiedener Kommunikationstopologien verwendet werden.

[1] https://www.5g-anbieter.info/verfuegbarkeit/5g-verfuegbarkeit-testen.html
[2] https://content.u-blox.com/sites/default/files/ShortRange-InternetOfThings_WhitePaper_%28UBX-14054570%29.pdf

Tabelle 2 vergleicht die heutzutage häufig verwendeten Bluetooth-Versionen v4.2 und v5.0.

Tabelle 2: Bluetooth v4.2 vs. v5.0

Version	Energieverbrauch	Datenrate	Reichweite
V4.0	1mW bis 10mW (Standby < 1mW)	Bis zu 1Mbps	Indoor 10 bis 30m Outdoor bis zu 100m
V4.2	1mW bis 15mW (Standby < 1mW)	Bis zu 1 Mbps	Indoor 10 bis 50m Outdoor bis zu 100m
V5.0	1mW bis 15 mW (Standby < 0.5mW)	bis zu 2 Mbps	Indoor 40 bis 100m Outdoor bis zu 240m

Bluetooth unterteilt sich in drei wesentliche Varianten: Bluetooth Classic (bis zur v4.2), Bluetooth Low Energy (BLE, v4.0 oder neuer) und iBeacon (basiert auf Bluetooth 4.0). Bei Classic arbeitet Bluetooth im 2,4GHz-ISM[3]-Band. Die Daten werden beim Senden zunächst fragmentiert und dann über einen der 79 verfügbaren Kanäle mit einer Bandbreite von 1 MHz übertragen. BLE als Erweiterung zum Bluetooth Classic zeichnet sich durch einen noch niedrigeren Energieverbrauch aus. Aus diesem Grund zielt diese Variante häufig auf kleine und energieeffiziente Geräte ab. Bei iBeacon handelt es sich um eine vereinfachte Version von BLE Classic, welche von Apple spezifiziert und zur Bluetooth-Kommunikation zwischen Apple-Produkten verwendet wird.

2.1.2.2 WLAN/802.11 und Low Power-Varianten

Wireless Local Area Network (WLAN) ist eine der am weitest verbreiteten drahtlosen Netzwerktechnologien und wird im Standard IEEE 802.11 auf physikalischer und Data Link-Ebene definiert. Für den Betrieb von WLAN wurden zwei ISM-Frequenzbereiche freigegeben, die lizenzfrei benutzt werden dürfen, 2,4 GHz und 5GHz. Verschiedene Umsetzungen dieses Standards existieren, die sich in Anzahl der Funkkanäle, Datenrate, Reichweite etc. unterscheiden. Für die meisten IoT-Anwendungen haben sich Geräte des Standards IEEE 802.11af, 802.11ah oder 802.11ba (siehe Tabelle 3) durchgesetzt, weil diese sich durch einen niedrigen Energieverbrauch auszeichnen[4], und im Frequenzbereich unter 1 GHz betrieben werden.

Tabelle 3: Übersicht häufig in IoT eingesetzter WLAN-Standards

	802.11af	802.11ah	802.11ba
Reichweite	Bis 3 km	Bis 1 km	Bis 1 km
Frequenz-Bereich	54 MHz bis 790 MHz	900 MHz bis 1 GHz	900 MHz bis 1 GHz
Max. Datenrate	35 Kbit/s	230 Mbit/s	230 Mbit/s

Bei Verwendung der WLAN-Protokolle im IoT sind bestimmte Vor- und Nachteile abzuwägen. WLAN zeichnet sich durch geringe Betriebskosten aus. Zudem ist der technische Aufwand für die Implementierung und Wartung einer WLAN-Infrastruktur relativ gering. Allerdings ist WLAN aufgrund des hohen Energieverbrauchs im Verhältnis zu anderen LPSRN für den Dauerbetrieb nicht für alle Szenarien die beste Wahl.

2.1.2.3 ZigBee und Thread

ZigBee ist ein Standard für drahtlose Verbindungstechnologien, der den IEEE 802.15.4-Standard insbesondere um die Möglichkeit des Routings und des sicheren Schlüsselaustausches erweitert. Ziel ist es, eine kostengünstige Verbindungstechnologie mit geringer Komplexität, geringem Stromverbrauch und

[3] Industrial, Scientific and Medical Band

[4] https://www.techtarget.com/searchnetworking/tip/Compare-low-power-Wi-Fi-protocols-and-their-roles-in-IoT

niedriger Datenübertragungsrate für den Einsatz in festen, tragbaren oder mobilen Geräten zu entwickeln.

Im 802.15.4-Standard sind zwei ISM-Bänder und DSSS-Bänder auf der physikalischen Schicht spezifiziert: 868 MHz bzw. 915 MHz mit einer Übertragungsrate von jeweils 20 Kbit/s bzw. 40 Kbit/s sowie 2,4 GHz mit einer Übertragungsrate von 250 Kbit/s. ZigBee definiert drei verschiedene Gerätetypen im Netzwerk: Koordinator, Router und Endgeräte. Der Router dient zum Austausch von Datenpaketen zwischen verschiedenen Endgeräten. Der Koordinator ist ein spezieller Typ von Router, der zusätzlich Netzwerke aktivieren kann. Beispielhafte Topologien sind in Abbildung 1 zu sehen. ZigBee wird dadurch geprägt, dass dieses Netzwerk selbstorganisierend ist und bis zu 65.000 Knotenpunkte gleichzeitig verwalten kann.

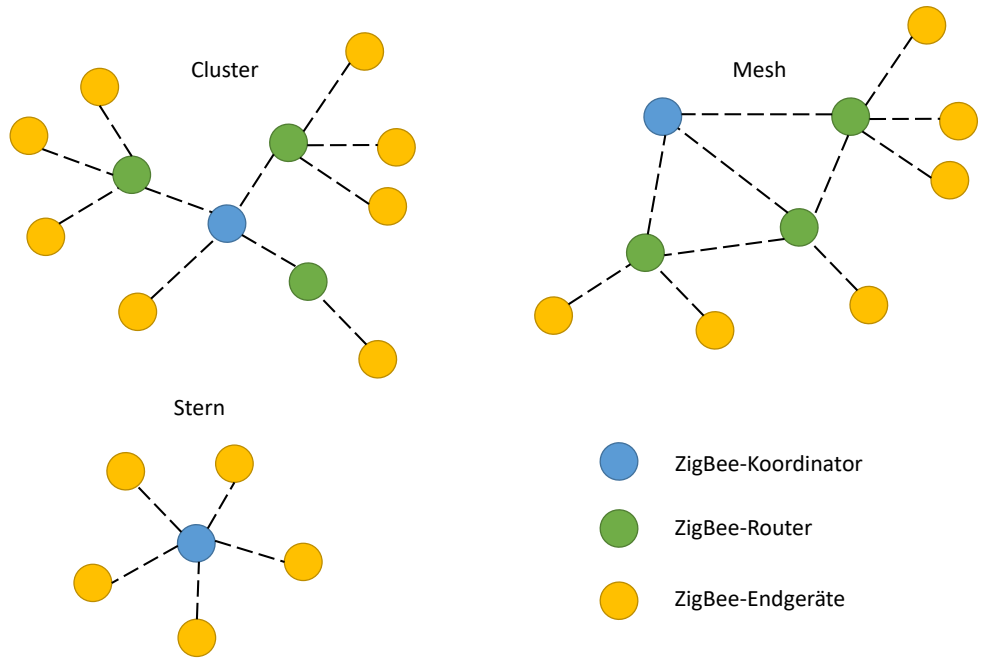

Abbildung 1: ZigBee-Topologien

Auf demselben Standard IEEE 802.15.4 wird die mit ZigBee vergleichbare Übertragungstechnologie namens Thread implementiert. Diese zielt darauf ab, Vernetzungen von IoT-fähigen Geräten im Bereich der Heimautomatisierung zu bewerkstelligen.[5]

Einer der Hauptunterschiede zwischen Thread und ZigBee ist, dass Thread das Internetprotokoll Version 6 (IPv6) nutzt, was eine direkte Verbindung zwischen Thread-Netzwerken und bestehenden IPv6-basierten Netzwerken wie WLAN ermöglicht. ZigBee ist hingegen nicht auf Basis von IPv6 entwickelt, sondern jeder Knoten im Netzwerk erhält eine 16-Bit-Adresse, die mithilfe eines Gateways in IP übersetzt werden muss.

Ein weiterer wichtiger Unterschied zwischen den beiden Standards liegt darin, dass Thread keine spezifischen Anwendungsschichten definiert, während ZigBee alle Schichten des OSI-Modells abdeckt. Dies macht Thread zu einer flexibleren Wahl in Bezug auf die Auswahl der Anwendungsschicht.

[5] Christoph Pallasch, 2019, "Kommunikationsinfrastruktur für den Cluster Wald und Holz", https://www.kwh40.de/wp-content/uploads/2019/11/KWH4.0_Standpunkt_Kommunikationsinfrastruktur_fuer_den_Cluster_Wald_und_Holz_v1.0.pdf

2.1.2.4 NFC und RFID

Near Field Communication (NFC) und Radio Frequency Identification (RFID) werden oft im selben Zusammenhang genannt. Beide Technologien basieren auf einem ähnlichen Prinzip und werden für die Kommunikation zwischen Geräten über sehr kurze Entfernungen (ca. bis 4 cm) genutzt.

Ein typisches RFID-System besteht aus einem Lesegerät und (mehreren) Tags, welche durch das Lesegerät gelesen werden, sobald sie sich diesem nähern. Weiterhin werden aktive und passive Tags unterschieden. Ein aktives Tag besitzt eine Stromversorgung und ist daher über mehrere Meter auslesbar. Ein passives Tag hingegen wird durch ein vom Lesegerät erzeugtes elektromagnetisches Feld mit Energie versorgt. Typische Anwendungsszenarien von RFID sind Logistik oder Proximity-Zugangskontrolle.

NFC unterscheidet sich von RFID dahingehend, dass ein bidirektionaler Austausch (Lesen und Schreiben) von Informationen zwischen zwei Geräten möglich ist. Wegen der kurzen Reichweite müssen sich die Geräte in unmittelbarer Nähe befinden. Dies ermöglicht eine sogenannte „physikalische Sicherheit", weshalb NFC oft für eine sichere Datenübertragung, z.B. das kontaktlose Bezahlen, eingesetzt wird.

Eine praktische Anwendung im Wald ist die Identifikation von Stammabschnitten.[6]

2.1.3 Low Power Wide Area-Netzwerke (LPWAN)

Low Power Wide Area-Netzwerk (LPWAN) steht für drahtlose Kommunikationstechnologien, die eine Datenübertragung zwischen vernetzten Geräten über große Entfernungen mit einer niedrigen Datenrate bei geringem Energiebedarf ermöglichen.

LPWAN wird häufig für Anwendungen in z.B. Smart City, Smart Grid, Energy Management oder Smart Manufacturing eingesetzt. Auch im WH-Sektor gibt es viele denkbare Beispiele der Nutzung:

- Ein Harvester steht weit entfernt von einem Forwarder, dem er einen Auftrag schicken soll – beide haben keine klassische IP-basierte Verbindung zum Internet. In dem Fall stehen typischerweise NB-IoT, Sigfox und LoRa zur Verfügung (siehe Kapitel 2.1.3.2 und 2.1.3.3).
- Ein Forwarder benötigt die Bodenfeuchte eines Waldbestands, welche durch einen Bodenfeuchtsensor gemessen und über LoRaWAN an den Forwarder übertragen wird.

In diesem Abschnitt wird eine Auswahl von Übertragungstechnologien in Kontext vom LPWAN vorgestellt.

2.1.3.1 LTE-M

Long Term Evolution for Machines (LTE-M) ist eine LPWAN-Technologie, die speziell für IoT-Anwendungen entwickelt wurde. Basierend auf dem 4G-LTE-Mobilfunkstandard bietet LTE-M eine kostengünstige, stromsparende und flächendeckende Lösung zur Vernetzung von IoT-Geräten. LTE-M ermöglicht eine Downlink-Datenrate von bis zu 1 Mbit/s und eine Uplink-Datenrate von bis zu 375 Kbit/s. Eine erweiterte Netzabdeckung wird durch ein Verbindungsbudget[7] von bis zu 40 dB gewährleistet. Diese Technologie bietet eine niedrige Übertragungslatenz von nur 5 ms. Außerdem unterstützt es Mobilität und Handover und bietet einen niedrigen Stromverbrauch mit einer Batterielebensdauer von bis zu 10 Jahren. Die Kommunikation erfolgt mit 128-Bit-AES-Verschlüsselung. Dies verbessert die IoT-Sicherheit.

[6] https://www.digitalmagazin.de/marken/forsttechnik/hauptheft/2021-7/Holzlogistik/044_rfid-bei-der-holzaufnahme

[7] Ein Verbindungsbudget (auch Link Budget) ist ein Maß für die Leistungsfähigkeit einer drahtlosen Kommunikationsverbindung. Es gibt an, wie viel Signalverlust zwischen Sender und Empfänger auftreten darf, damit die Verbindung noch funktioniert.

2.1.3.2 NB-IoT

Narrow Band-IoT (NB-IoT) ist speziell für „low-cost“ und „long-range“ IoT vorgesehen. Diese Verbindungstechnologie basiert auf Funktechnologie mit einer auf 200 kHz beschränkten, lizenzierten Bandbreite und setzt auf vorhandene Mobilfunknetze (daher in 3rd Generation Partnership Project (3GPP) für Cellular-Geräte standardisiert) auf. NB-IoT ermöglicht eine Maximalgeschwindigkeit im Downlink von 234,7 kbit/s und im Uplink von 204,8 kbit/s sowie eine max. Reichweite bis 35 km.

NB-IoT kann durch Aufrüstung bestehender Cellular-Netze umgesetzt werden. Auf dieser Grundlage kann NB-IoT auch Bereiche, in denen Mobilfunkempfang nicht immer verfügbar ist (z.B. Tiefgaragen oder Keller), abdecken.

2.1.3.3 Sigfox und LoRa

Sigfox (proprietär) und LoRa (offen) sind wesentliche LPWAN-Ansätze und haben ähnliche fundamentale Prinzipien und Architekturen. Aus diesem Grund werden sie in diesem Abschnitt zusammengefasst und verglichen. Der Fokus liegt dabei auf den Aspekten Geschäftsmodell, Netzwerkarchitektur und Funktionsprinzip.

Sigfox ist ein Unternehmen, welches sich mit dem Betrieb eines LPWAN-Netzwerks beschäftigt und eine eigene IoT-Lösung als Network as a Service (NaaS) in rund 57 Ländern insb. zur Vernetzung von „low-power“-Objekten anbietet. Das Geschäftsmodell von Sigfox definiert, dass sich Sigfox-Nutzer nur um die Endgeräte kümmern, während die Firma Sigfox den Betrieb und die Verwaltung einer Infrastruktur anbietet.

Long Range (LoRa) ist ebenfalls eine LPWAN-Funktechnologie, die auf der physikalischen Schicht definiert wird. LoRaWAN nutzt LoRa und ergänzt dies um ein Kommunikationsprotokoll und eine Systemarchitektur für das Netzwerk. Nach aktuellem Stand ist LoRa in rund 100 Ländern im Einsatz. Nutzer können insbesondere das Netzwerk des LPWAN-Anbieters The Things Network[8] verwenden bzw. dessen Infrastruktur über eigene Gateways erweitern. Alternativ kann eine eigene LoRaWAN-Infrastruktur z.B. auf Basis von Chirpstack[9] aufgebaut werden.

In Hinblick auf die technische Architektur sind beide Netzwerke ähnlich aufgebaut. Diese Architektur kann generell in vier Schichten unterteilt werden. In der ersten Schicht (physikalische Schicht) befinden sich Endgeräte, die sich um Datenerfassung und -sammlung kümmern. Die Rohdaten werden im Anschluss an die Gateways oder Router weitergeleitet, die in der zweiten Schicht befinden sind. Auf der dritten Schicht stehen diverse Netzwerkserver, die die Daten empfangen, verarbeiten und speichern. Endnutzer (letzte Schicht) greifen auf die Daten zu und realisieren so IoT-Anwendungen.

Beide Technologien nutzen dieselben lizenzfreien ISM-Bänder (868 MHz in Europa). Im Sigfox-Netzwerk erfolgt die bidirektionale Kommunikation zwischen Endgeräten und Gateways (auch Basisstationen genannt) über die Binary Phase-Shift Keying (BPSK)-Modulation. Bei LoRa wird ebenfalls eine bidirektionale Kommunikation unterstützt, die durch Chirp Spread Spectrum (CSS) moduliert wird. Ein technischer Vergleich ist in Tabelle 4 dargestellt.

Tabelle 4: Technischer Unterschied zwischen Sigfox und LoRa(WAN)

Verbindungs-technologie	Max. Anzahl der Nachrichten		Max. Größe der Nachricht [Byte]		Sicherheit	Reichweite [km]	
	Uplink	Downlink	Uplink	Downlink		Rural	Urban
Sigfox	140/Tag	4/Tag	12	8	AES-128	30-50	3-10

[8] https://www.thethingsnetwork.org/
[9] https://www.chirpstack.io/

	7/Stunde						
LoRa	84/Tag	12/Tag		256	Abhängig von Anbieter; bei TTN z.B. AES-128	15-20	2-5

In einem IoT sind weitere Aspekte wie Quality of Service (QoS) oder Energieverbrauch relevant. Ein weiterer Vergleich zwischen LoRaWAN und Sigfox ist in Adorno et al.[10] zu finden.

2.1.4 Vergleich

Dieses Kapitel bietet eine Übersicht über die Verbindungstechnologien in LPSRN und LPWAN, die in vielen mobilen Geräten direkt nutzbar bzw. umsetzbar sind. Mit Fokus auf den Vergleich des Energieverbrauchs und der Reichweite werden alle vorgestellten Protokolle in Abbildung 2 noch einmal zusammengefasst. Die dargestellte Reichweite und der Energieverbrauch können abhängig vom konkreten Design des Kommunikationsnetzwerks variieren. Daher ist diese Abbildung nur als Anhaltspunkt zu betrachten.

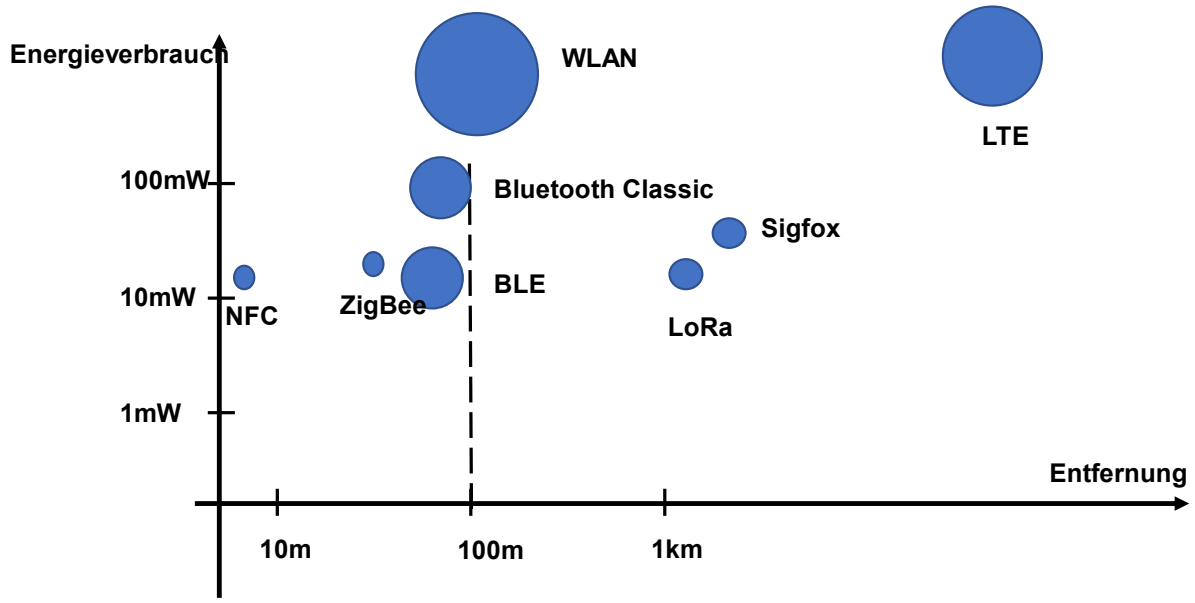

Abbildung 2: Verbindungstechnologien in LPSRN und LPWAN mit Reichweite und Energieverbrauch

In der Praxis ist die Netzwerk-Kommunikation im Wald komplexer, da hier weitere Aspekte betrachtet werden müssen, z.B. ob der Funk reflektiert und somit gedämpft wird oder ob die Kommunikation durch schlechtes Wetter beeinflusst wird.

2.2 Ad-hoc-Netzwerke

Ein drahtloses Ad-hoc-Netzwerk ist ein dezentrales Netzwerk bestehend aus mehreren mobilen Knoten, welches nicht auf eine bestehende Kommunikationsinfrastruktur angewiesen ist. Daher sind in der Regel keine Router oder Zugriffspunkte vorhanden. Das Routing von Daten wird stattdessen durch einzelne Knoten ermöglicht, die anhand verschiedener Protokolle miteinander kooperieren. Die Topologie eines Ad-hoc-Netzwerks kann dynamisch gestaltet werden, da die Randbedingungen der Szenarien sich ändern können und Knoten und Netzwerk schnell angepasst werden müssen. Ansätze für Ad-hoc-Netzwerke können auf verschiedenen Funktechnologien basieren. Oft wird dazu WLAN eingesetzt.

[10] D. Adorno et.al, Evaluation of LP-WAN Technologies for Fire Forest Detection Systems, ALLSENSORS 2019

2.2.1 Routing

Ein wichtiger Baustein im Ad-hoc-Netzwerk ist das Routing, weil es direkt das Verhalten der Datenweiterleitung zwischen verschiedenen Knoten (Route) und damit auch die Performance bestimmt. Es gibt viele Forschungsarbeiten[11,12] auf dem Gebiet der Entwicklung und Auswertung verschiedener Routing-Protokolle. Die folgenden Eigenschaften stehen im Mittelpunkt[13]:

- Routen-Entdeckung
- Routen-Auswahl
- Routen-Wartung
- Datenweiterleitung
- Routen-Repräsentation und Metrik

Ziel der Routen-Entdeckung ist die Identifikation aller potenziell möglichen Routen zum Zielknoten. Entsprechende Protokolle unterteilen sich in die Gruppen proaktiv, reaktiv und hybrid.

Eine geeignete Route soll nach dem Schritt „Routen-Entdeckung" selektiert werden. Hierfür gibt es quell- sowie zielknotenorientierte Methoden. Diese unterscheiden sich darin, ob die Entscheidung der Routen-Auswahl beim Quell- oder Zielknoten getroffen wird.

Die Routen-Wartung bezieht sich auf die kontinuierliche Überprüfung der Gültigkeit der ausgewählten Route, d.h. ob ein Datenpaket diese durchlaufen kann. Die Datenweiterleitung (also die Weiterleitung von Datenpaketen zwischen verschiedenen Knoten) ist generell abhängig von der Netzwerkkapazität und dem genutzten Protokoll.

Die Routen-Repräsentation beschreibt, wie Informationen über die Route interpretiert bzw. gespeichert werden können. Als Metrik können verschiedene Parameter zur Auswertung der Route zur Verfügung stehen, die mathematisch minimiert werden können. Klassische Parameter sind z.B. Entfernung, Latenzzeit und Kanalrauschen, die das Routing maßgeblich beeinflussen können.

2.2.2 Klassifikation

Jeder Knoten verwaltet lokal in einer Tabelle Informationen über Topologie und Routing. Verschiedene Klassen ergeben sich danach, wie diese Tabelle im jeweiligen Knoten aktualisiert wird. Im Allgemeinen lassen sich drahtlose Ad-hoc-Netzwerke einer der unten beschriebenen Klassen zuordnen.

2.2.2.1 Proaktive Routing-Protokolle

In einem proaktiven Routing-Protokoll ist es ständige Aufgabe jedes Knotens, die eigene Tabelle mit den Informationen über Topologie und Routing aktuell zu halten. Diese Informationen werden im gesamten Netzwerk durch den „Link-State"- oder den „Distance-Vector"-Ansatz verbreitet.

Bei „Link-State" informiert jeder Knoten alle anderen Knoten im Netzwerk über seine direkten Nachbarn durch Flooding. Dies findet nur statt, wenn sich eine Änderung der Tabelle ergibt. Im Vergleich dazu gibt jeder Knoten bei „Distance-Vector" sein Wissen über das gesamte Netzwerk an seine Nachbarn weiter – und aktualisiert seine eigene Tabelle entsprechend auf Basis der Informationen seiner Nachbarn. Der Austausch erfolgt mit einem vordefinierten Zeitintervall.

---

[11] Al-Dhief, F. T., Sabri, N., Fouad, S., Latiff, N. A., & Albader, M. A. A. (2019). A review of forest fire surveillance technologies: Mobile ad-hoc network routing protocols perspective. *Journal of King Saud University-Computer and Information Sciences*, *31*(2), 135-146.

[12] Alotaibi, E., & Mukherjee, B. (2012). A survey on routing algorithms for wireless ad-hoc and mesh networks. *Computer networks*, *56*(2), 940-965.

[13] Lee, M. J., Zheng, J., Hu, X., Juan, H. H., Zhu, C., Liu, Y., ... & Saadawi, T. N. (2006). A new taxonomy of routing algorithms for wireless mobile ad hoc networks: the component approach. *IEEE Communications Magazine*, *44*(11), 116-123.

2.2.2.2 Reaktive Routing-Protokolle

In einem reaktiven Routing-Protokoll initiiert der Absenderknoten den Suchprozess nach einer passenden Route zum Zielknoten. So ist das Routing mit einem geringeren Overhead verbunden, weil Routen erst nach Bedarf (on-demand) ermittelt werden. D.h. eine ständige Aktualisierung der Routentabellen ist hier nicht mehr erforderlich.

2.2.2.3 Hybride Routing-Protokolle

Hybride Routing-Protokolle kombinieren den „Distance-Vector"- und „Link-State"-Ansatz. Die Informationen über die Route werden durch Flooding verbreitet, sobald sich die Topologie des Netzwerks ändert. Hybrid-Routing ermöglicht damit eine schnelle Konvergenz und erfordert weniger Rechenleistung und Speicherplatz des Netzwerks.

2.2.3 Vergleich

Die Routing-Verfahren für drahtlose Ad-hoc-Netze werden nach zentral/dezentral und proaktiv/reaktiv klassifiziert, ähnlich wie für drahtgebundene Netzwerke. Die Algorithmen wurden in den letzten Jahren zwecks besserer Umsetzbarkeit in verschiedenen Szenarien weiterentwickelt und neue Routing-Kategorien wurden eingeführt. Eine Zusammenfassung der Verfahren ist in Paper[14] zu sehen. In dieser Übersicht werden Ad-hoc-Netzwerke insbesondere nach den folgenden Aspekten klassifiziert:

- Geographie: Kommunikation erfolgt in Abhängigkeit von geographischen Positionsinformationen. Datenpakete werden an einen geographischen Standort statt an eine Netzadresse geschickt
- Geo-Casting: Zustellung von Datenpaketen nur an eine Teilmenge von Zielen, die durch die geographische Lage statt Netzadresse identifiziert sind
- Hierarchie: Routing von Datenpaketen beruht auf hierarchischer Adressierung
- Multiroute: Routing-Technik, bei der mehrere alternative Pfade durch ein Netz gleichzeitig genutzt werden

In drahtlosen Netzwerken ist Ad-hoc eine der Betriebsarten für Funkarten, die in 802.11 standardisiert sind. Die Kommunikation findet nur auf der ersten OSI-Schicht – der physikalischen Schicht – statt. Im Grunde genommen kann jedes Gerät mit allen anderen Geräten kommunizieren, solange die Funkreichweite dies erlaubt. Insbesondere im Infrastrukturmodus können drahtlose Geräte nur mit einem zentralen Access Point oder Router kommunizieren, welche sich dann um die Weiterleitung von Datenpaketen an den nächsten Knoten (Client) kümmern. In Ad-hoc-Netzwerken werden Access Points nicht mehr berücksichtigt. Dies bedeutet, wenn Gerät A ein Gerät B erreichen kann und gleichzeitig Gerät B ein Gerät C erreichen kann, können A und C nicht unbedingt kommunizieren, weil B keine Pakete weiterleiten kann. In Mesh-Netzwerken findet die Kommunikation auf der dritten OSI-Schicht – der Netzwerkschicht – statt. Mesh ermöglicht es jedem Gerät im Netzwerk als Router zu fungieren und Pakete im Namen anderer Geräte weiterzuleiten.

2.3 Kommunikationsprotokolle

Auf Basis der einzelnen Verbindungstechnologien werden Kommunikationsprotokolle realisiert, worüber die Kommunikation möglichst unabhängig von Geräten oder Gateways im IoT erfolgen soll. Ziel der Nutzung von Protokollen ist es, einen Datenaustausch zwischen mehreren Kommunikationsteilnehmern auf technischer Ebene zu ermöglichen.

Im IoT-Kontext stehen diverse Kommunikationsprotokolle zur Verfügung. In diesem Abschnitt werden einige Protokolle der Anwendungsschicht und Transportschicht nach dem ISO/OSI-Sieben-Schichten-

[14] Alotaibi, Eiman, and Biswanath Mukherjee. "A survey on routing algorithms for wireless ad-hoc and mesh networks." Computer networks 56.2 (2012): 940-965.

modell (siehe Abbildung 3) zusammengefasst, die im IoT-Bereich häufig genutzt werden. Die klassischen Protokolle aus der Bitübertragungsschicht und Sicherungsschicht, die auf verschiedenen Funktechnologien basieren, wurden bereits in Kapitel 2.1 eingeführt.

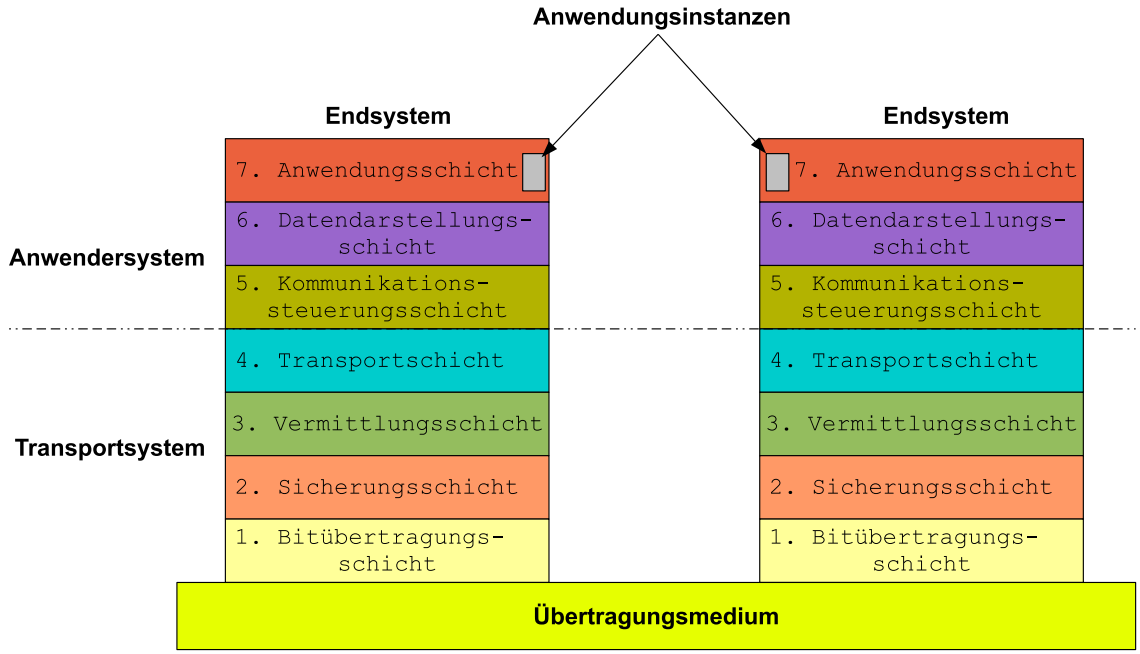

Abbildung 3: ISO/OSI Modell[15]

2.3.1 Transportschicht

2.3.1.1 TCP

TCP steht für „Transmission Control Protocol“, ein Kommunikationsstandard der es Anwendungen und Geräten ermöglicht, Nachrichten über Netzwerke verbindungsorientiert auszutauschen, wodurch eine erfolgreiche Zustellung von Daten und Nachrichten gewährleistet werden kann.

TCP als einer der grundlegenden Standards, der die Basis für viele Kommunikationsprotokolle auf der Anwendungsschicht bereitstellt, ist eines der an den häufigsten verwendeten Protokolle in verschiedenen Domänen. In einem klassischen TCP-Netzwerk umfasst die Topologie immer einen Server und einen Client. Der Austausch erfolgt nach dem Server-Client-Muster. Vor der Datenübertragung initiiert der Client einen Verbindungsaufbau mit dem Server durch das sogenannte „Handshaking“, mit dessen Hilfe sich Sender und Empfänger beim Verbindungsaufbau ihre Nachrichten gegenseitig bestätigen. Eine ähnliche Phase wird auch beim Verbindungsabbau durchgeführt. TCP ermöglicht eine zuverlässige, geordnete und fehlergeprüfte Datenübertragung und wird in IoT-Anwendungen in der Regel im Kontext der Protokolle HTTP(S), MQTT, AMQP und weiteren eingesetzt.

2.3.1.2 UDP

Das User Datagram Protocol (UDP) bezeichnet ein Kommunikationsprotokoll, das sich dadurch auszeichnet, Verbindungen zwischen Geräten und Maschinen mit geringer Latenz und Verlusttoleranz über Netzwerke herzustellen. Die verbindungslose Kommunikation in UDP erfolgt ebenso nach dem Server-Client-Muster und ermöglicht eine schnelle Übertragungsrate, weil vor dem Datenaustausch keine Verbindungsaufbauphase zwischen den Kommunikationspartnern erforderlich ist. Daher ist dieses Protokoll bei zeitkritischer Kommunikation vorteilhaft, z.B. Voice over IP.

[15] https://de.m.wikipedia.org/wiki/Datei:ISO-OSI-7-Schichten-Modell%28in_Deutsch%29.svg (Urheber: Deadlyhappen; CC BY-SA 4.0; unverändert)

Im IoT-Kontext zeichnet es sich im Vergleich zu TCP durch seine Eigenschaften für die folgenden Anwendungsszenarien besonders aus:

- Geräte mit beschränkten Ressourcen
- Übertragung mit geringer Datenrate im Downlink
- „Low-Power“-Applikationen

UDP ist zwar einfach zu implementieren und hat weniger Overhead, macht die Applikationen bzw. Geräte aber auch anfälliger für Cyberangriffe.

2.3.2 Anwendungsschicht

2.3.2.1 MQTT

MQTT ist eine Abkürzung für „Message Queuing Telemetry Transport“ – ein Protokoll, das für Netzwerke mit geringer Bandbreite und Geräte mit beschränkten Ressourcen und hoher Latenz spezialisiert ist. In einem klassischen MQTT-Modell (siehe Abbildung 4) gibt es diverse Clients und einen zentralen Broker, die auf unterschiedlichen Maschinen betrieben werden können. Die Kommunikation erfolgt nach dem Publisher-Subscriber-Pattern. Absender und Empfänger werden dabei nicht unmittelbar miteinander verbunden, sondern die auszutauschenden Daten (Nachrichten) werden durch den Publisher im zentralen Broker veröffentlicht, wo sie mit einem bestimmen Topic assoziiert sind. Subscriber, die sich mit dem Broker auf dem entsprechenden Topic verbinden, holen sie dort ab.

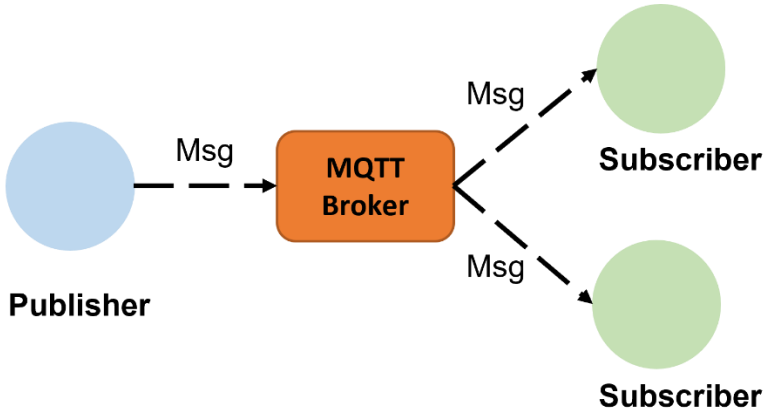

Abbildung 4: Kommunikation in MQTT

2.3.2.2 AMQP

AMQP steht für „Advanced Message Queuing Protocol“, ein Open-Source-Protokoll für Nachrichtenorientierte Middlewares. Ziel der Nutzung dieses Protokolls ist, die Sequenzierung und Weiterleitung (sowohl peer-to-peer als auch publish-subscribe) von Nachrichten zu ermöglichen.

Im AMQP-Modell (siehe Abbildung 5) werden Absender und Empfänger über einen zentralen Broker verbunden, der eine (oder mehrere) „Exchange(s)“ zur Weiterleitung der Nachrichten sowie diverse „Queues“ als Zwischenspeicher enthält. Die Exchange wird mit einer (oder mehreren) Queue(s) durch einen „Binding (Routing Key)“ verknüpft. Beim Senden wählt der Absender über das Binding den Adressaten der Nachricht.

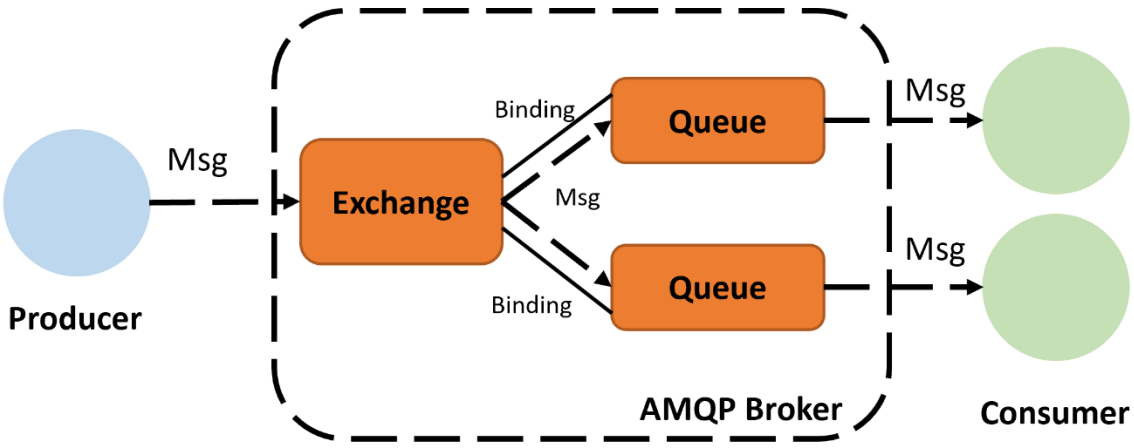

Abbildung 5: Kommunikation in AMQP

2.3.2.3 HTTP

Das Hypertext Transfer Protocol (HTTP) ist ein Server-Client-basiertes Kommunikationsprotokoll auf der Anwendungsschicht zur zustandslosen Datenübertragung, d.h. der Server speichert keine Zustände von beliebigen Requests/Responses und wird nur vom Client „angesprochen". HTTP nutzt hauptsächlich TCP/IP auf der Transportschicht, wobei die Kommunikation typischerweise durch Transport Layer Security (TLS) verschlüsselt werden kann (HTTPS).

HTTP wird häufig mit Representational State Transfer (REST) kombiniert genutzt. Eine REST-basierte Architektur beschreibt Bedingungen, unter denen Application Programing Interfaces (APIs) funktionieren. Eine „RESTful"-API stellt dazu die HTTP-Methoden GET, PUT, POST, DELETE und weitere zur Interaktion mit Ressourcen auf einem Webserver zur Verfügung. Dazu verweist der Entwurfsstil von REST-API auf Eigenschaften[16], die beim Server implementiert werden sollen.

2.3.2.4 CoAP

CoAP (Constrained Application Protocol) ist ein leichtgewichtiges Protokoll, welches speziell für die Informationsübertragung zwischen Web-basierten Anwendungen insb. auch im IoT entwickelt wird. Es basiert auf dem Server-Client-Modell und ermöglicht Geräten mit begrenzten Ressourcen effizient miteinander zu kommunizieren.

CoAP verwendet eine REST-Architektur ähnlich wie HTTP. Damit ist eine Kommunikation mit den Methoden u.a. GET, PUT, POST, und DELETE auch unterstützt. Die native Integration von UDP ermöglicht CoAP schnelle Übertragungen, welche daher auch weniger ressourcenintensiv sind.

2.3.2.5 Websocket

Das Websocket-Protokoll ist ein auf TCP basierendes Kommunikationsprotokoll zur bidirektionalen Verbindung zwischen einer Webanwendung und einem Websocket-Server. Websocket ist kompatibel mit HTTP. Allerdings unterscheiden sich Websocket von HTTP in der Gestaltung der Interaktion zwischen Server und Client. Bei Websocket kann die Kommunikation sowohl vom Server als auch vom Client initiiert werden, sodass sich der Client aktiv und kontinuierliche über Zustandsänderungen vom Server informieren lassen kann, ohne selbst immer wieder nachzufragen (Polling).

2.3.2.6 OPC UA

OPC UA ist die Weiterentwicklung des Standards Open Platform Communications (OPC) der OPC Foundation und ist ein Kommunikationsprotokoll zum Datenaustausch für industrielle Anwendungen. Es

[16] https://learn.microsoft.com/en-us/azure/architecture/best-practices/api-design

erlaubt den sicheren und zuverlässigen Zugriff auf Maschinen, Geräte und Systeme von unterschiedlichen Herstellern.

Im Vergleich zu anderen IoT-Protokollen, wie z.B. MQTT und AMQP, ermöglicht OPC UA, durch Informationsmodelle die Prozessdaten einer Maschine mit einer semantischen Beschreibung zu erweitern. Die Kommunikation erfolgt nach dem Server-Client-Pattern. D.h. der OPC-Standard wird direkt auf einer Maschine implementiert und stellt genormte Schnittstelle nach außen bereit. Im Inneren befinden sich die gerätespezifischen Protokolle zur Steuerung der Maschine. OPC UA ermöglicht eine Plattformunabhängigkeit durch die Abkehr von COM/DCOM hin zu rein binärer TCP/IP oder alternativ SOAP-Kommunikation[17].

2.3.2.7 Vergleich

Eine Übersicht über die IoT-Protokolle der Anwendungsschicht, die heutzutage häufig genutzt werden, wird in Tabelle 5 aufgeführt.

Tabelle 5: Übersicht über IoT-Protokolle der Anwendungsschicht

	MQTT	CoAP	AMQP	HTTP	Websocket	OPC UA
Transport-protokoll	TCP	UDP	TCP	TCP	TCP	TCP
Pattern	Pub/Sub	Pub/Sub and Req/Res	Pub/Sub and Req/Res	Req/Res		Server/Client
QoS	QoS 0 (at most once) QoS 1 (at least once) QoS 2 (exactly once)	Nein	QoS 0 (at most once) QoS 1 (at least once) QoS 2(exactly once)	Nein	Nein	Nein
Security	TLS/SSL	DTLS	TLS/SSL	SSL	TLS/SSL	Spezifischer Algorithmus zum Schlüsselaustausch
Encoding	Binär	Binär	Binär	Text	Binär	Binär
RESTful unterstützt	Nein	Ja	Nein	Ja	Ja	Ja[18]

2.4 Informationsdatenmodelle

Heterogene Prozesse und Systeme in der Forstwirtschaft führten zu einer hohen Diversität der verwendeten Datenformate. Dies verhindert einen durchgängigen, interoperablen Datenaustausch entlang der Wertschöpfungsketten der Forstwirtschaft. Das Standpunktpapier „Datenstandards in Wald und Holz 4.0" des KWH4.0[19] gibt eine Übersicht der existierenden Standards sowie deren Einordnung in die Prozesskette. Im Folgenden sind die für Smart Forestry relevanten Standards zusammengefasst.

[17] https://www.opc-router.de/was-ist-opc-ua/

[18] Grüner, S., Pfrommer, J., & Palm, F. (2016). RESTful industrial communication with OPC UA. IEEE Transactions on Industrial Informatics, 12(5), 1832-1841.

[19] Thomas Gerritzen, Ariane Kuchta, 2020: Datenstandards in Wald und Holz 4.0, https://www.kwh40.de/wp-content/uploads/2020/03/Standpunkt_Datenstandards_Wald_Holz40_v1.0.pdf

2.4.1 StanForD[20]

Der internationale Industriestandard StanForD (Standard for machine data and communication) wurde 1990 für Forstmaschinendaten eingeführt, um z.B. zwischen Harvester und Forwarder unterschiedlicher Hersteller Daten auszutauschen. Der ursprüngliche Standard (mittlerweile häufig „StanForD classic“ genannt) basierte auf einem binären „Kermit“-Protokoll und umfasste verschiedene Dateitypen u.a. für Objektbeschreibungen, Aushaltungsinstruktionen oder Produktionsdateien. Obwohl es sich um einen Industriestandard handelte, war es dennoch nicht immer möglich, Daten verschiedener Hersteller untereinander auszutauschen und korrekt zu verstehen. Dies und weitere Aspekte führten zur Entwicklung des moderneren XML-basierten „StanForD2010“ Standards. Obwohl StanForD2010 seit über 10 Jahren eingeführt ist, fahren insbesondere in Deutschland noch viele Maschinen mit dem alten Standard. Die Aufgaben des Standards umfassen, die Daten aus der Holzernte von und zwischen Forstmaschinen interoperabel auszutauschen, um damit Kontrolle, Berichterstellung und Überwachung/Nachverfolgung der Holzernteprozesse zu ermöglichen. StanForD2010 definiert verschiedene Datenformate für verschiedene Aspekte der Holzernte, insbesondere Harvesting Production Report (HPR) sowie Forwarding Production Report (FPR) für zentrale Produktinformationen, Product Instruction (PIN), Object Instruction (OIN) sowie Species Group Instruction (SPI) für Auftragsdaten an den Harvester und Forwarding Object Instruction (FOI) sowie Forwarding Delivery Instruction (FDI) für Auftragsdaten an das Rückefahrzeug.

2.4.2 ELDAT und ELDATSmart

ELDAT wurde als Datenstandard für die Holz- und Forstwirtschaft in Deutschland entwickelt. Das Ziel ist das Ersetzen der papierbasierten Kommunikation durch standardisierte und automatisierte Prozesse. Der ursprüngliche Standard wird heute als ELDATclassic bezeichnet. ELDAT wurde im Laufe der Zeit zu ELDATsmart weiterentwickelt. Seit der Unterzeichnung der *Rahmenvereinbarung für ELDAT* 2018 ist ELDATsmart der Branchenstandard für die Übertragung von Daten zwischen Akteuren der Holz- und Forstwirtschaft in Deutschland.

ELDATsmart umfasst fünf Hauptfunktionen: Die Holzbereitstellung, den Transportauftrag, den Lieferschein, das Wald- bzw. Werksmaßprotokoll und die Abrechnung. In der Holzbereitstellung bietet der Waldbesitzer sein Holz zum Verkauf an bzw. meldet die Bereitstellung des geschlagenen Holzes. Das Sägewerk sendet den Transportauftrag an ein Fuhrunternehmen. Der Lieferschein enthält alle relevanten Adress- und Kontaktdaten, sowie Informationen zu Herkunft, Umfang und Art der Ladung. Das Messprotokoll hält Details zur Vermessung des Holzes fest. Die Abrechnung enthält alle Daten, die zur Abwicklung des Zahlungsvorgangs notwendig sind (Bankdaten, steuerliche Informationen, Kontakte, Holzdaten etc.).

Laut einer Umfrage aus dem Jahr 2022[21] benutzen alle Landesforstbetriebe inklusive der Bundesforste mindestens einen der beiden ELDAT-Standards. Dabei nutzen 40% ausschließlich ELDATclassic, 13% ausschließlich ELDATsmart und die restlichen 47% beide Versionen. Zwar variiert die Nutzung der einzelnen Module stark, doch insgesamt ist der Standard in der Branche weit verbreitet.

2.4.3 PapiNet

PapiNet[22] ist ein internationaler Datenstandard, welcher ursprünglich von und für die Papierindustrie entwickelt wurde. Im Laufe der Zeit wurde der Standard auf andere Bereiche innerhalb der Forst- und

[20] https://www.skogforsk.se/english/projects/stanford/stanford-2010/

[21] Kaulen und Oberwalleney 2022: Implementierung des ELDAT Standard in den Forstbetrieben in Deutschland. https://kwf2020.kwf-online.de/wp-content/uploads/2022/07/2022_Implementierung-des-ELDAT-Standard-in-den-Forstbetrieben-in-Deutschland_AKDO.pdf

[22] http://www.papinet.org/

Holzwirtschaft ausgeweitet. Ziel des Standards ist eine schnelle und einheitliche Kommunikation zwischen Akteuren der Branche, um den Informationsfluss sicherzustellen.

2.4.4 FHPDAT[23] [24]

FHPDAT ist das österreichische Pendant zum deutschen ELDAT Standard. Er beschreibt den elektronischen Datenaustausch zwischen den Bereichen Säge, Industrie und Logistik. Sein Ziel ist die Steigerung des Informationsaustausches zur Planung und Steuerung der Geschäftsprozesse in der Forst- und Holzwirtschaft. FHPDAT ist XML-basiert und in vier Module aufgeteilt.

2.4.5 DRMDat

DRMDat[25, 26] entstand als jüngster Standard aus einem österreichisch-deutschen Verbundvorhaben. DRMDat vereint die Funktionen von ELDATsmart und FHPDAT. Ziel war ein Standard zum Warenaustausch zwischen Deutschland und Österreich. DRMDat beinhaltet mehr Module als ELDATsmart. Neben weiteren Modulen rund um die Holzlogistikkette sind Module zur Forsteinrichtung und Maßnahmenerhebung geplant.

3 Kommunikationstechnologien bei Herstellern

Vernetzung ist ein grundlegender Baustein für die Digitalisierung der Kommunikation und der realisierten Prozesse. Viele Hersteller von Forstmaschinen und handgeführten Geräten verfolgen diese Prinzipien bereits. Fokus ist hier aber oftmals ein geschlossenes Ökosystem. Dieser Abschnitt gibt einen Überblick und Vergleich.

3.1 Forstmaschinen

Viele Maschinenhersteller bieten ähnliche Kommunikationskonzepte an. Diese unterscheiden unter anderem die externe Kommunikation („Wie kann ich mich mit anderen Maschinen und Apps verbinden?“) und die interne Kommunikation („Wie können die Daten zwischen verschiedenen Modulen innerhalb einer Maschine ausgetauscht werden?“). Weitere Aspekte sind z.B. Datenmodelle, Kommunikationsprotokolle etc.:

- Welche Software/Programme werden zur Kommunikation genutzt?
- Mit welcher Hardware (insb. Sensoren) werden Maschinen ausgerüstet?
- Welche Funktechnologien werden als Grundlage zur Kommunikation eingesetzt?
- Welche Vernetzungstechnologien werden zur Kommunikation genutzt?
- Welche Protokolle werden zur Kommunikation genutzt?
- Welche Datenmodelle stehen zur Verfügung?

Diese Fragestellungen wurden für die drei Anbieter Ponsse, Johne Deere und Komatsu Forest im Jahr 2021 und 2022 untersucht. Tabelle 6 zeigt die Ergebnisse.

Tabelle 6: Übersicht über die Kommunikationsarchitekturen bei Maschinenherstellern

Hersteller	Ponsse	John Deere	Komatsu
Maschinen-typen	Harvester, Forwarder	Harvester, Forwarder	Harvester, Forwarder

[23] https://www.forstholzpapier.at/fhpdat
[24] https://www.forstholzpapier.at/fhpdat/reader
[25] https://kwf2020.kwf-online.de/portfolio/drmdat/
[26] https://www.drmdat.eu/

Hardware / Sensoren	Bordcomputer: Intel i5-7442 EQ, SSD, GSM Sensoren: GPS-Modul Drucksensoren Temperatursensoren Beschleunigungssensoren Orientierungssensoren	Bordcomputer mit GPS- und MTG 4G LTE-Modul Sensoren nach Kundenspezifikation, z.B. Sensoren für die Kippstabilität	Bordcomputer: Intel Celeron J1900, 2.0/2.41Ghz (Quad Core) Sensoren: Smart Crane[27]
Software/ Programme	Harvester-Steuerungssoftware: OPTI4G, OPTI5G[28], Harvester Active Crane[29] Kundenspezifische Software, z.B. Zeiterfassungssysteme Cloudspeicher[30], z.B. mit Bosch IoT insights[31] Mailsoftware[32] Forwarder-Steuerungssoftware: Opti Control-Rückezugsystem[33]	TimberMatic, TimberMaticMaps (Windows-basiert), TimberManager (webbasiert bzw. Cloud-basiert), Intelligente Kransteuerung IBC[34]	Steuerungs-systeme: MaxiXTGIS[35] Programme: MaxiVision[36], MaxiFleet
Funktechnologien	LTE/Bluetooth/WLAN/Communication Unit GSM	LTE/Bluetooth/WLAN/Communication Unit GSM	LTE/WLAN
Technologien zur internen Vernetzung	ARCNET (Bordcomputer zu Modulen)[37] CAN (Module zu Sensoren/Aktoren)	CAN: Kommunikation zwischen Steuerungseinheiten und Modulen	Diverse CAN-Kreise für interne Maschinenkommunikation
Datenmodelle	Maschineneinstellungsdatei in einer PONSSE-proprietären SQL-Datenbank StanForD2010-Format	StanForD2010-Format	StanForD2010-Format

Die Kommunikationsarchitekturen, die bei den drei Maschinenherstellern jeweils für große Forstmaschinen wie Harvester und Forwarder genutzt werden, ähneln sich. Alle untersuchten Forstmaschinen sind mit einem Bordcomputer ausgestattet, auf dem in der Regel ein Windows-Betriebssystem und eine Hersteller-spezifische Software zur Steuerung bzw. Monitoring der Maschine installiert sind.

[27] Dies ist eine intelligente Kranspitzsteuerung, welche durch den Einsatz von Sensoren neue Möglichkeiten bei der Kransteuerung bietet

[28] https://www.ponsse.com/de/produkte/informationssysteme/produkte/-/p/harvester_systems#/

[29] https://wahlersforsttechnik.de/die-neue-generation-harvester/

[30] Mit dem Cloudspeicher können Daten zwischen den Maschinen und dem Büro synchronisiert werden. Seit 2021 in der Ponsse Deutschland Cloud)

[31] https://www.boschrexroth.com/de/de/blog/transparente-forstmaschine-ponsse-verbessert-after-sales-service-mit-iot/

[32] Mit der Mailsoftware werden z.B. die Maschinendaten (Harvesterprotokolle, Volumen, Zeiten etc.) verschickt oder Arbeitsanweisungen empfangen

[33] https://www.ponsse.com/de/produkte/informationssysteme/produkte/-/p/forwarder_systems#/

[34] https://www.deere.de/de/forstmaschinen/ibc/

[35] https://www.komatsuforest.de/forstmaschinen/kontroll-und-informationssystem

[36] https://www.komatsuforest.de/media/news/komatsu-forest-pr%C3%A4sentiert-maxivision

Zur Kommunikation zwischen internen Komponenten/Modulen von Forstmaschinen wird häufig ein geschlossener CAN-Bus eingesetzt. CAN hat sich als Standard-Bus-System im Kraftfahrzeugbereich durchgesetzt.

Zur Interaktion mit anderen Maschinen werden in der Regel diverse Funktechnologien genutzt, die sich weiterhin in „Long Range“ (z.B. LTE/4G/3G) und „Short Range“ (z.B. Bluetooth, WLAN) unterteilen. Die ausgegebenen Daten werden im StanForD2010- bzw. proprietären Format umgesetzt. Diese werden meistens zwischen Maschinen desselben Herstellers ausgetauscht.

3.2 Handgeführte Geräte

Als Beispiel für Kommunikationstechnologien bei handgeführten Geräten in der Forstwirtschaft wird in diesem Abschnitt eine Übersicht der Cloud-Architektur von STIHL vorgestellt (Abbildung 6).

Abbildung 6: STIHL-Systemübersicht der Cloud-Architektur[38]

Die Cloud-Architektur lässt sich auf ein klassisches IoT-Drei-Schichten-Modell abbilden, dass sich in „Perception Layer“, „Network Layer“ und „Application Layer“ aufteilt. Auf der untersten Ebene befinden sich einzelne physische Assets mit den zugehörigen Sensoren. Sie bilden zusammen ein lokales Netzwerk, in dem die Maschinen- und Produktionsdaten per Bluetooth miteinander ausgetauscht und an ein Gateway übermittelt werden. Im Network Layer werden die übertragenen Daten durch das Gateway in die STIHL-Cloud weitergeleitet. Ein Beispiel-Gateway ist die STIHL Connected (mobile) Box, die mit verschiedenen Netzwerkvarianten (WLAN, Ethernet) und Mobilfunkvarianten (2G/3G/4G) ausgestattet ist. Im Application Layer werden Anwendungen realisiert, über die diese Daten aus der Cloud abgerufen, analysiert, verarbeitet und visualisiert werden können.

3.3 Zusammenfassung

Digitale Vernetzung ist bei fast allen Maschinenherstellern ein relevantes Thema. Aktuell wird sie jedoch durch folgendes maßgeblich beschränkt:

- Die Kommunikation zwischen den Komponenten/Modulen innerhalb einer Forstmaschine erfolgt meistens über einen geschlossenen und internen CAN-Kreis. Dadurch ist kein (Direkt-)Zugriff von außen auf Steuerungsgeräte sowie IO-Komponenten der Maschine möglich. Dies wird aktuell, wenn überhaupt, nur über Hersteller-eigene Plattformen ermöglicht, was zu technischen Silos führt, die nur eingeschränkt mit anderen Systemen vernetzbar sind.
- Ebenso ist der Datenaustausch zwischen Forstmaschinen bislang maßgeblich innerhalb des Ökosystems desselben Herstellers möglich.
- Darüber hinaus bieten viele Maschinenhersteller proprietäre Cloud-Lösungen, die z.B. REST-Schnittstellen zur Kommunikation bereitstellen. Allerdings wird u.a. aus IT-Sicherheitsgründen

[38] Bild aus STIHL connected: digitales Gerätemanagement | STIHL (Urheber: Stihl, unverändert)

bei vielen kein Zugriff für Anwendungen Dritter erlaubt. Beispielsweise ist aktuell keine solche Abfrage der Daten in der STIHL-Cloud vorgesehen.

4 Kommunikationsinfrastrukturen in der Praxis

Dieses Kapitel befasst sich mit Kommunikationsarchitekturen bei verschiedenen Forschungsprojekten oder industriellen Anwendungsfällen, die mit den Randbedingungen der intelligenten und clusterübergreifend integrierten Holzernte vergleichbar sind.

4.1 FeltGIS

FeltGIS[39] ist eine norwegische Firma, die sich mit technischen Lösungen für die Vernetzung in der Forstwirtschaft beschäftigt. Das Produkt „FeltBox“ ermöglicht einen echtzeitnahen drahtlosen Datenaustauch via WLAN in einem lokalen Netzwerk zwischen Akteuren, Forstmaschinen sowie allen anderen relevanten Objekten, die mit einer FeltBox ausgerüstet sind. Außerdem ermöglicht die FeltBox eine Verbindung zum Internet. In dem Fall können Daten auch an andere FeltBoxen übertragen werden, die in anderen weit entfernten Netzwerken sind.

Die „FeltLog“-App ermöglicht eine bidirektionale Interaktion mit den FeltBoxen unter einer definierten Berechtigung und zeigt relevante Informationen an. Die App ermöglicht Forstmaschinenführern, Auftragsdaten bzw. Karten oder Produktionsdaten, die von Maschinen erzeugt werden, zu erhalten. Dabei werden die Produktionsdaten dann via LTE/3G in eine zentrale Datenbank hochgeladen.

4.2 LogBuch (Treeva)

LogBuch[40] befasst sich mit digitalen Lösungen zur vernetzten Baum- und Grünflächenerfassung im Wald. Die grundlegende Kommunikationsarchitektur nutzt eine Kombination aus Sprachaufzeichnung und Bluetooth zur freihändigen, georeferenzierten Aufnahme von Informationen über Bäume, Planung, Arbeitsabläufe, usw. Die aufgezeichnete Sprache wird zusammen mit den Metadaten (insbesondere der Georeferenzierung) in eine zentrale Stelle synchronisiert und dort automatisch analysiert und klassifiziert. Die abgeleiteten Informationen können als Karte oder Tabelle in georeferenzierten Formaten (xlsm, Geojson, shp, GPX) exportiert werden.

4.3 Smart Systems Service Infrastructure (S³I)

Die Smart Systems Service Infrastructure (S³I)[41] wurde durch das Kompetenzzentrum Wald und Holz 4.0 (KWH4.0) in Kooperation mit dem FNR-geförderten Vorhaben iWald zur dezentralen Vernetzung in einem forstlichen Internet der Dinge (Internet of Things, IoT) entwickelt. Die zu vernetzenden sogenannten „Wald und Holz 4.0-Dinge“ (WH4.0-Dinge) umfassen dabei (vgl. Abbildung 8):

- WH4.0-Komponenten, d.h. physische Assets wie Forstmaschinen, Sensoren, Waldbestände oder Forstwirte in Kombination mit ihrem jeweiligen Digitalen Zwilling, also ihrem Abbild in der Informationswelt,
- WH4.0-Dienste zur Bereitstellung übergreifender Funktionalitäten wie z.B. Waldwachstumssimulation oder Predictive Maintenance und
- WH4.0-Mensch-Maschine-Schnittstellen (WH4.0-MMS), d.h. insbesondere mobile Apps oder Desktop-Anwendungen.

WH4.0-Dinge können dabei durch verschiedene Ansätze umgesetzt werden, was zu einer hohen technischen Heterogenität führt. Digitale Zwillinge können ihre Laufzeitumgebung beispielsweise direkt auf einem Computer auf dem betroffenen Asset haben (Edge-Ansatz), auf einem Server (Cloud-Ansatz)

[39] https://www.feltgis.no/en/
[40] https://treeva.de/
[41] M. Hoppen 2020, „Konzeption und Einsatz der Smart Systems Service Infrastructure (S³I) zur dezentralen Vernetzung in Wald und Holz 4.0“, https://www.kwh40.de/wp-content/uploads/2020/04/KWH40-Standpunkt-S3I-v2.0.pdf.

betrieben werden oder es gibt gemischte Ansätze (Fog-Ansatz). Ein Harvester wird einen Digitalen Zwilling nach dem Edge- oder Fog-Ansatz wählen, weil Daten lokal erfasst und vorverarbeitet werden müssen und der Digitale Zwilling auch ohne Verbindung zum Internet vor Ort bspw. in einem Ad-hoc-Netzwerk erreichbar sein soll. Demgegenüber wird der Digitale Zwilling eines Waldbestands maßgeblich in einer Cloud verwaltet werden. Darüber hinaus gibt es eine organisatorische Heterogenität, weil Akteure ihre WH4.0-Dinge typischerweise nicht auf einer einzigen zentralen Plattform betreiben, sondern ihre eigene Wahl treffen wollen (Plattform-Skepsis, Vendor-Lock-in). Zudem zeigt sich bei der Vernetzung in der Forstwirtschaft die besondere Anforderung, dass WH4.0-Dinge im Unterschied zum klassischen IoT nicht immer über das Internet erreichbar sind (z.B. Forstmaschinen im Einsatz), so dass eine Pufferung von Nachrichten notwendig ist.

Auf dieser Grundlage wurde die S³I als minimale zentrale IoT-Infrastruktur entwickelt, die aus den folgenden Komponenten besteht (Abbildung 7):

- S³I-IdentityProvider: Verwaltet die Identitäten der WH4.0-Dinge und stellt ihnen dazu einen OAuth 2.0-konformen Dienst zur Authentifikation (Single-Sign-On) bereit
- S³I-Directory: Speichert die Metadaten der WH4.0-Dinge und stellt einen REST- sowie Websocket-konformen Abfragedienst bereit, der eine Rollen-basierte Zugriffskontrolle unterstützt
- S³I-Broker (optional) zum AMQP-basierten, Ende-zu-Ende-verschlüsselten Nachrichtenaustausch nach dem Store-and-Forward-Prinzip
- S³I-Repository (optional) als Cloud-Speicher für die Daten der WH4.0-Dinge selbst
- S³I-Registration: Dienst zur REST-konformen Konfiguration/Registrierung der WH4.0-Dinge

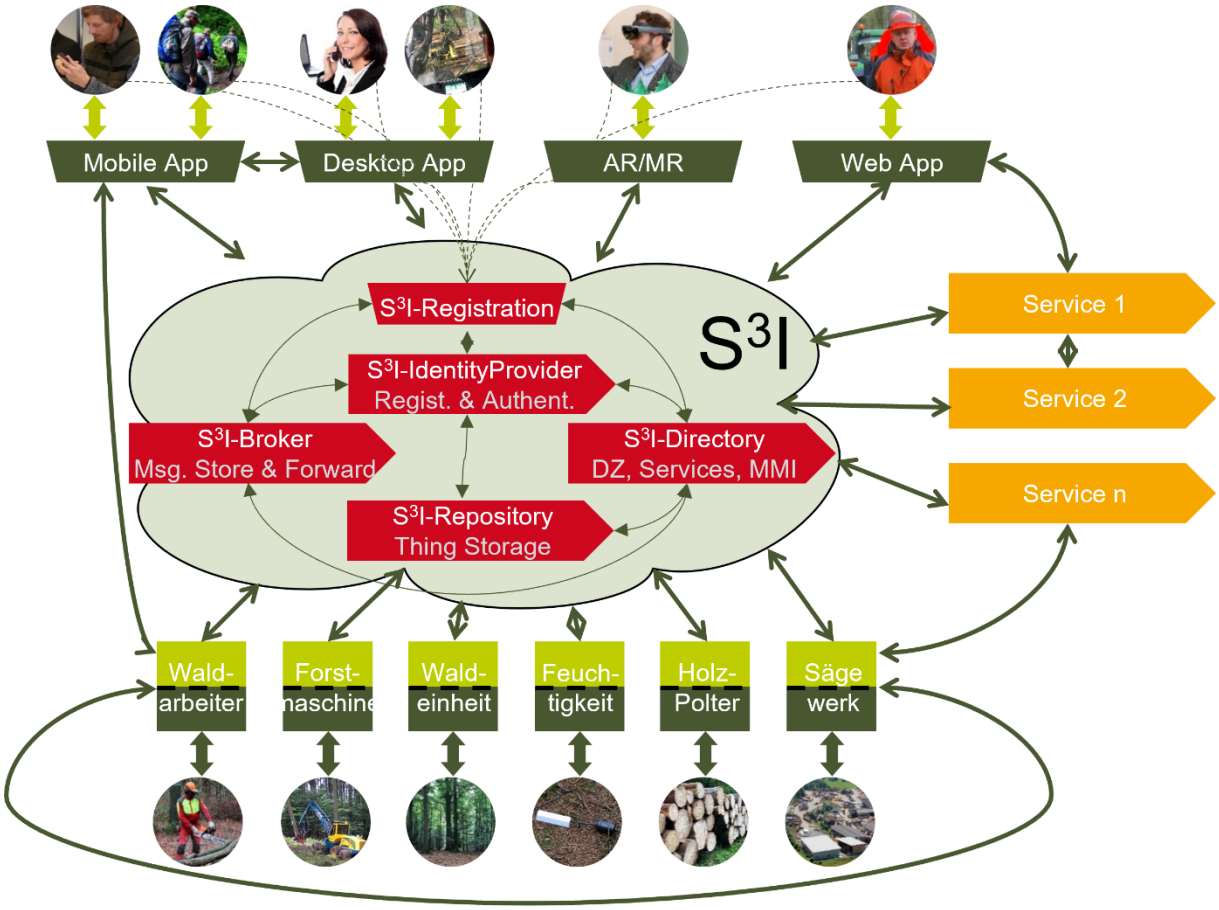

Abbildung 7: Grundkonzept „Smart Systems Service Infrastructure“[42]

4.4 DEMETER

Moderne Technologien zur Digitalisierung und Vernetzung werden bereits länger in der Landwirtschaft eingesetzt. In diesem Kontext gibt es z.B. Forschungsprojekte wie SmartFarming[43] oder Smart Agriculture[44]. Voraussetzung für eine erfolgreiche Digitalisierung ist die Vernetzung der einzelnen Bausteine. Dies erfordert den Einsatz von IoT-Technologien. Beispiele in diesem Bereich sind Agrirouter[45] und DEMETER[46]. Im vorliegenden Kapitel wird auf das Projekt DEMETER eingegangen.

4.4.1 Hintergrund

Das Horizon 2020-Projekt DEMETER (09/2019-08/2023) befasste sich mit der Entwicklung und Umsetzung einer IoT-basierten Smart Farming-Plattform über 18 Länder. Ziel des Projekts war es, die digitale Transformation in der Agrar- und Ernährungswirtschaft durch die Integration u.a. von IoT-Technologien, Datenwissenschaft und intelligenter Landwirtschaft auf EU-Ebene einzuführen.

4.4.2 Komponenten

Eine der größten Hindernisse bei der Einführung von Smart Farming-Lösungen ist die generell fehlende Konnektivität und Interoperabilität zwischen verschiedenen Systemen und Plattformen im Agrar- und Ernährungssektor, insb. zwischen denen der Technologieanbieter. Damit ist die Situation mit der in der

[42] Fotos: (o.) A. Böhm, RIF; Rainer Sturm / pixelio; Konstantin Gastmann / pixelio; Stefan Wein, WZL; A. Böhm; Peter Kamp / pixelio; (u.) A. Böhm; HSM; S. Wein; A. Böhm; S. Wein; Michael Lorenzet / pixelio

[43] https://dmexco.com/de/stories/smart-farming/

[44] https://smart-agriculture.org/de/

[45] https://agrirouter.com/de/

[46] https://h2020-demeter.eu/

Forstwirtschaft vergleichbar. DEMETER versucht, diese Lücke der technischen und semantischen Interoperabilität durch Bereitstellung einer Menge von Interoperabilitätsmechanismen und eine gemeinsame (semantische) Sprache zu füllen. Dies soll durch eine zentrale Systemarchitektur ermöglicht werden[47].

4.4.2.1 Agricultural Interoperability Space (AIS)

Der Agricultural Interoperability Space (AIS) stellt eine Menge von Interoperabilitätsmechanismen und Tools zur Entwicklung, Validierung sowie Umsetzung der DEMETER-Lösung bereit. Das heißt, alle in DEMETER registrierten Entitäten werden mit den Tools des AIS ausgerüstet, um dadurch DEMETER-fähig zu werden. Dies ermöglicht eine standardisierte Schnittstelle der DEMETER-Entitäten.

4.4.2.2 Brokerage Service Environment (BSE)

Das Brokerage Service Environment (BSE) stellt einen Dienst zur Registrierung, Entdeckung sowie Kommunikation zwischen allen in DEMETER agierenden Akteuren, Applikationen, Diensten usw. in einer sicheren Art und Weise dar. Das BSE wird dazu von jeder mit DEMETER-Technologien ausgestatteten Entität (DEMETER Enhanced Entity, DEE) zur Authentifizierung genutzt. Dadurch ist die authentifizierte Entität von anderen registrierten DEEs entdeckbar.

In DEMETER wird ein föderiertes Konzept umgesetzt. Es wird eine zentrale BSE-Komponente bereitgestellt. Unabhängig davon kann jede Ausführungsplattform eine eigene BSE-Komponente zugewiesen bekommen, mit der sich die DEEs sowohl innerhalb der Ausführungsplattform als auch außerhalb authentifizieren können.

4.4.2.3 Agricultural Information Model (AIM)

Das Agricultural Information Model (AIM) ist ein umfangreiches Informationsmodell bestehend aus einem Meta-Datenmodell zur Beschreibung verschiedener Devices und Systeme, die über DEMETER miteinander vernetzt werden und einer Ontologie zur semantischen Beschreibung der auszutauschenden Daten zwecks Interoperabilität.

4.4.2.4 DEMETER Enabler Hub (DEH)

Als Kernmodul der DEMETER-Architektur dient der DEMETER Enabler Hub (DEH) zur zentralen Speicherung der AIM-konformen Beschreibung aller Demeter-Entitäten bestehend aus Komponenten, Geräten, Diensten, Datenquellen, Plattformen usw.

Im DEH werden Endnutzer weiter gruppiert als DEMETER-Provider und/oder DEMETER-Consumer. Provider können ihre Ressourcen anbieten, während Consumer den DEMETER-Katalog durchsuchen und geeignete Ressource nach ihrer Anforderung finden können. Die in DEH gehosteten Ressourcen sind über Web-Schnittstellen und REST-APIs erreichbar.

4.4.2.5 Access Control System (ACS)

Das Access Control System (ACS) kümmert sich um Autorisierung in der zentralen DEMETER-Cloud, d.h. Zugriff auf den zentralen BSE und DEH.

4.4.3 Vergleich mit S³I

DEMETER ist gut vergleichbar mit der S³I. Tabelle 7 illustriert die grundlegenden Unterschiede zwischen den beiden Infrastrukturen. Der wesentliche Unterschied liegt darin, dass in DEMETER jede Ausführungsplattform ein einziges BSE zugewiesen bekommt, bei dem sich alle Devices oder Applikationen, die mit DEE DEMETER-konform ausgerüstet werden und sich in derselben Ausführungsplattform befinden, authentifizieren, gegenseitig finden und kommunizieren können. Eine deutliche Beschränkung

[47] Demeter Reference Architecture (Release 1), 28/02/2020, https://h2020-demeter.eu/wp-content/uploads/2020/10/D3.1-DEMETER-reference-architecture_v1.0.pdf

ist, dass in DEMETER kein lokaler Datenaustausch vorgesehen ist sondern der Fokus auf Cloud-basierter Datenbereitstellung liegt.

Tabelle 7: Vergleich zwischen DEMETER und S³I

DEMETER-Komponente	Vergleichbare Komponente in S³I	Anmerkungen
DEH	S³I-Directory ohne Access Control System	Beides sind zentrale Komponenten, in denen Metadaten gehostet werden und über Webschnittstelle erreichbar sind.
AIS	N.A.	Bereitstellung standardisierter Mechanismen / Schnittstellen für Endnutzer, um einen Direktzugriff auf DEH zu ermöglichen. Tools zur Erstellung DEMETER-fähiger Applikationen, Services und Ressourcen.
ACS	Access Control in allen zentralen S³I-Diensten	Zentrale Verwaltung der Entitäten- sowie User-Berechtigungen
BSE	S³I-Broker + S³I-Config + S³I-IdentityProvider	Ermöglicht eine lokale, remote sowie Cloud-basierte Vernetzung von DEEs
N.A.	S³I-Repository	In Demeter müssen Repositories individuell umgesetzt werden
Dashboard	S³I-Manager + UI zur Client-Konfiguration	Dashboard hat Direktzugriff auf SOCS, AIS und ACS.

5 Kommunikationsarchitektur für Smart Forestry

Die im KWH4.0 entwickelten Wald und Holz 4.0-Konzepte in Verbindung mit IoT-Ansätzen bieten Lösungsstrategien zur grundlegenden Kommunikation in Wald und Holz. Damit soll eine Verbesserung der Digitalisierung, Vernetzung und Prozessautomatisierung für die Wertschöpfungsketten der Holzernte ermöglicht werden. Hierfür liefert Smart Forestry die notwendige Architektur und Standards auf Basis bestehender WH4.0-Konzepte zur dezentralen Vernetzung.

5.1 Gesamtarchitektur

Grundlage der Kommunikationsarchitektur sind die bestehenden Konzepte, Methoden und Technologien von Wald und Holz 4.0 und dabei insbesondere die S³I. Diese werden unter Berücksichtigung der identifizierten Anforderungen der intelligenten und clusterübergreifend integrierten Holzernte geschärft und vervollständigt.

Abbildung 8 zeigt, wie WH4.0-Dinge (vgl. Kapitel 4.3) über eine zentrale IoT-Infrastruktur vernetzt werden können. Diese Vernetzung erfolgt unabhängig von konkreten Ausführungsplattformen, z.B. wo WH4.0-Dinge (insbesondere Digitale Zwillinge) betrieben werden oder „leben“. Auch entlang der Holzerntekette agieren unterschiedlichste Akteure, die typischerweise eine eigene Wahl bei der Umsetzung ihrer Systeme treffen möchten. Abgesehen davon sind technische Ansätze zur Realisierung der WH4.0-Dinge unterschiedlich. Auch von dieser Heterogenität ist die Vernetzung unabhängig. Allerdings müssen in diesem Kontext WH4.0-Dinge mit einem standardisierten Interface ausgestattet werden.

Während WH4.0-Dinge selbst dezentral verteilt sind erfolgt ihre Vernetzung und Kommunikation über eine zentrale bzw. globale S³I-Instanz. Im Vergleich dazu ermöglichen dezentrale Ansätze mehr Pri-

vatsphäre und Autonomie. Darüber hinaus sind dezentrale Systeme widerstandsfähiger gegen Datenverluste oder Hardwareausfälle (Single Point of Failure[48]), da die Daten, insbesondere sensitive Identitätsdaten, dezentral oder auf mehrere Knoten verteilt gespeichert werden können. Ein weiterer technischer Grund in Bezug auf forstliche Anwendungsszenarien besteht in der oft schlechten Mobilfunkverfügbarkeit im Wald insbesondere in Deutschland, sodass eine Verbindung mit einer zentralen IoT-Infrastruktur nicht durchgängig möglich ist. Somit wurde in Smart Forestry eine weitergehende, schrittweise Dezentralisierung der Kommunikation umgesetzt.

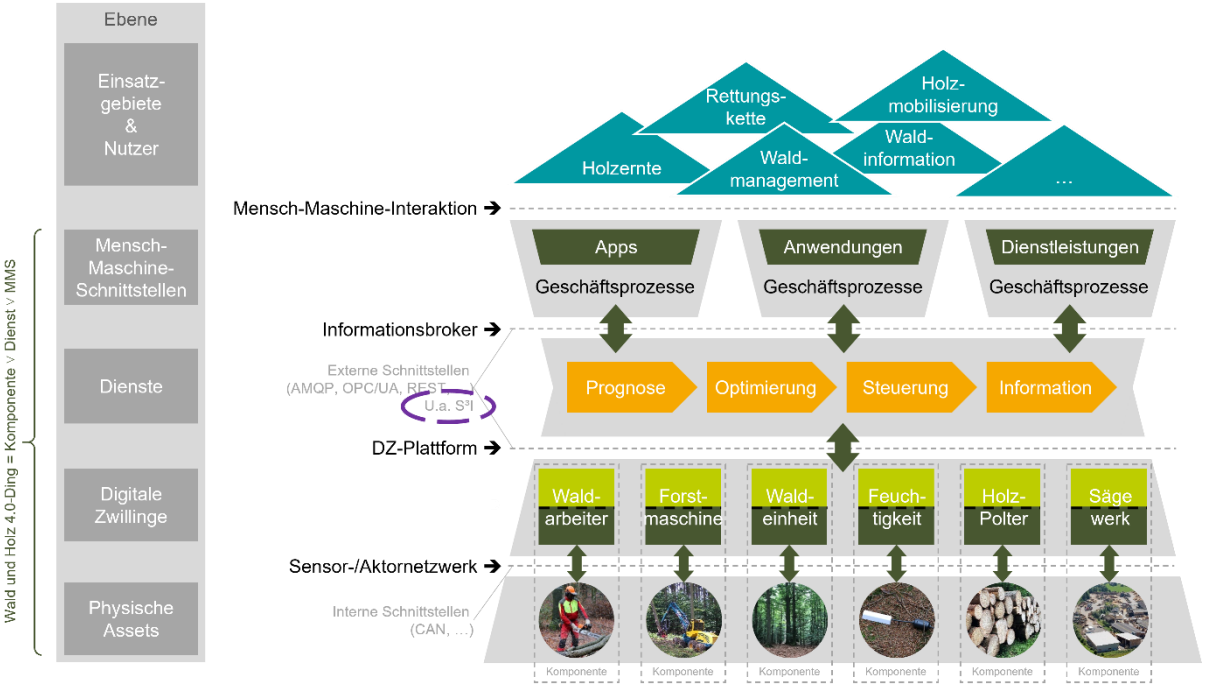

Abbildung 8: Vernetzung der „Dinge“ in Wald und Holz 4.0[49]

Abbildung 9 illustriert das erarbeitete Konzept für eine lokal zentralisierte, global dezentralisierte Kommunikationsarchitektur für Smart Forestry. Wesentliche Komponenten in diesem Konzept sind eine globale S³I-Infrastruktur (oben) kombiniert mit mehreren lokalen S³I-Infrastrukturen (unten). Die Vernetzung innerhalb einer lokalen S³I-Infrastruktur lässt sich dabei ad-hoc oder klassisch (Infrastruktur mit Router) aufbauen. Bedarfsorientiert kann einer Organisation oder einem Einsatz (z.B. motormanueller Holzernteeinsatz) eine lokale S³I-Infrastruktur zugewiesen werden. Damit wird eine lokale, IoT-Kommunikation zwischen den in der Infrastruktur vernetzten WH4.0-Dingen realisiert, auch wenn im Einsatzgebiet kein Mobilfunk verfügbar ist. Darüber hinaus können lokale S³I-Infrastrukturen mit einem Internetzugang ausgestattet werden, über den ein Zugriff von außen auf die dortigen WH4.0-

[48] https://www.techtarget.com/searchdatacenter/definition/Single-point-of-failure-SPOF

[49] Aufbauend auf Bosch Software Innovations 2012. Fotos (v. l.): A. Böhm, RIF; HSM; S. Wein, WZL; A. Böhm; S. Wein; Michael Lorenzet / pixelio

Dinge ermöglicht wird. Aus diesem Grund wird das Konzept als „lokal zentralisiert, global dezentralisiert“ bezeichnet.

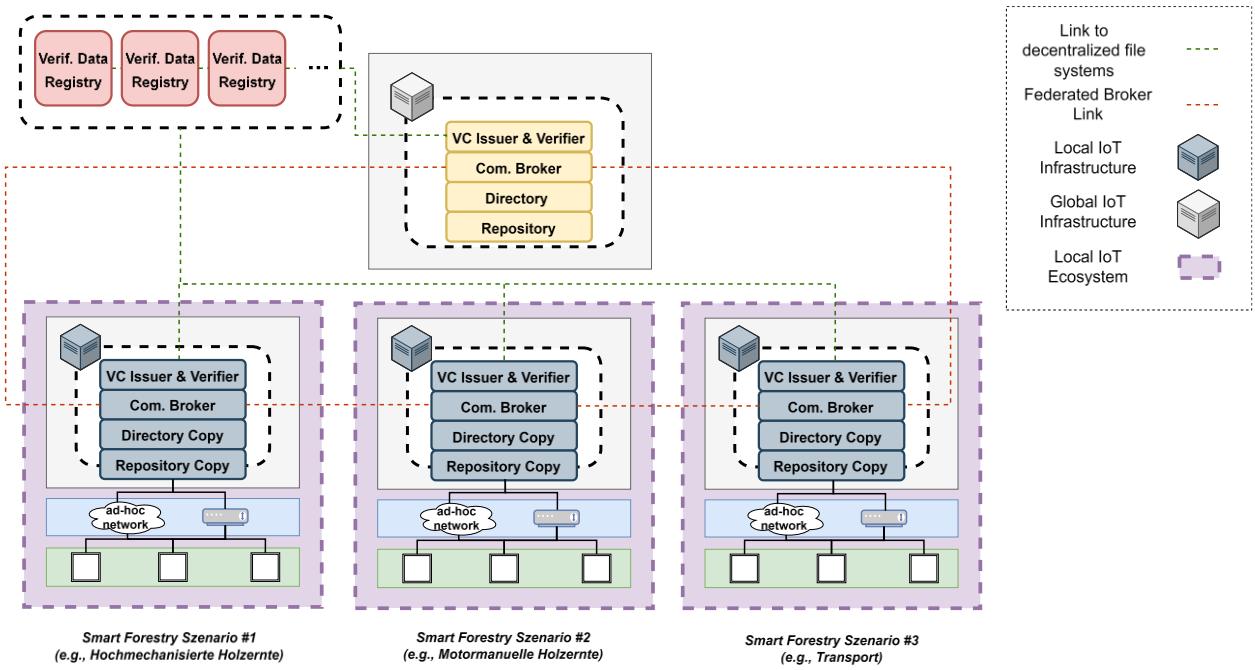

Abbildung 9: Gesamte Kommunikationsarchitektur für Smart Forestry

5.2 Kommunikationsinfrastrukturen

Die in diesem Abschnitt diskutierten Kommunikationsinfrastrukturen vernetzen alle WH4.0-Dinge über lokale bzw. globale S³I-Infrastrukturen. Die Vernetzung innerhalb eines WH4.0-Dings, z.B. die Kommunikation zwischen einem Harvester-Kopf und dem Bordcomputer oder allgemein die Vernetzung zwischen dem Asset und seinem Digitalen Zwilling, wird dabei nicht betrachtet und erfolgt individuell. Wie im vorherigen erwähnt, besteht die Gesamtarchitektur aus einer globalen und mehreren lokalen IoT-Infrastrukturen. Die infrastruktur-übergreifende Vernetzung von WH4.0-Dingen hängt von der Vernetzung dieser Infrastrukturen untereinander ab. Dieser Abschnitt fokussiert daher darauf,

- wie WH4.0-Dinge zwischen globaler und lokalen S³I-Infrastrukturen miteinander vernetzt werden und
- wie die lokalen Infrastrukturen konzeptuell realisiert werden.

Lokale S³I-Infrastrukturen können z.B. auf einer „S³I-Box“ umgesetzt werden, welche u.a. einen Mini-Rechner (z.B. Raspberry Pi 4) und ein Spannungsversorgungsmodul umfasst, siehe Abbildung 10. Lokale S³I-Infrastrukturen können ebenso auf Servern teilnehmender Institutionen betrieben werden, um so deren Souveränität zu erhöhen.

Abbildung 10: Hardware-Laufzeitumgebung für lokale S³I-Infrastruktur („S³I-Box“)

5.2.1 Vernetzung von globalen und lokalen Infrastrukturen

Konzeptuell setzen sich beide (globale und lokale) Infrastrukturen aus denselben Komponenten zusammen. Authentifizierung und Autorisierung erfolgen über die Konzepte „Decentralized Identifier (DID)[50]“ und „Verifiable Credential (VC)[51]“ des W3C[52]. DID ist eine Realisierung von Self-Sovereign Identity (SSI)[53] und zielt auf eine volle Kontrolle über die Identität sowie der darauf bezogenen Informationen ab. Mit einem DID lässt sich ein VC ausstellen und einem WH4.0-Ding zuweisen, welcher dann – wie der Name besagt – verifizierbare Attribute zusammenstellt und anderen zur weiteren Überprüfung (z.B. Access Control) zur Verfügung stellt. Beispiel 1 zeigt ein VC, welcher als ein Alumni-Zertifikat agiert. In dem VC ist das Attribut „Example University“ durch die Methode „RSASignature2018“ verifizierbar gemacht.

Zur Kommunikation wird weiterhin das Store & Forward-Konzept basierend auf dem AMQP-Protokoll verwendet. Ein Directory-Dienst dient dem Speichern der Metainformation der WH4.0-Dinge und ein optionaler Repository-Dienst als Datenspeicher für Cloud-/Fog-basierte DZ.

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "AlumniCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }]
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.edu/issuers/565049#key-1",
  }
}
```

Beispiel 1: Ein Verifiable Credential dient als Alumni-Zertifikat[54]

[50] https://www.w3.org/TR/did-core/
[51] https://www.w3.org/TR/vc-data-model-2.0/
[52] Im Rahmen des Forschungsprojekts wurde die Authentifizierung und Autorisierung mit dem klassischen OpenID Connect umgesetzt
[53] https://norbert-pohlmann.com/glossar-cyber-sicherheit/self-sovereign-identity-ssi/
[54] Beispiel direkt kopiert aus dem W3C VC Data Model v1.1, https://www.w3.org/TR/vc-data-model/

5.2.1.1 Registrierung im globalen S³I

Auch ein lokales S³I selbst braucht eine eindeutige Identität, die es vom globalen S³I zugewiesen bekommt. Diese wird für den Aufbau des Vertrauens zwischen VC Issuer und Verifier der beiden S³I (global und lokal) genutzt. Abbildung 11 zeigt den verallgemeinerten Prozess.

Der Prozess beginnt mit einer Registrierungs-Anfrage an die globale S³I-Infrastruktur (Schritt 1). Diese Anfrage löst die weiteren Schritte zur Erstellung der Infrastrukturidentität sowie eines Directory-Eintrags für die Metainformationen der Infrastruktur (Schritt 2) aus. Die anzulegende Identität der lokalen Infrastruktur wird in der Liste der vertrauenswürdigen Instanzen des globalen S³I eingetragen. So wird das Vertrauen zwischen den beiden Instanzen etabliert. In dem Zusammenhang wird eine instanzenübergreifende Verifikation von DIDs und VCs ermöglicht, auch wenn die VCs aus einer anderen S³I-Infrastruktur ausgestellt werden. Eine entsprechende Antwort auf die Anfrage im Schritt 1 stellt das Ergebnis der Registrierung dar. Im Schritt 4 kann das lokale S³I anschließend konfiguriert und genutzt werden.

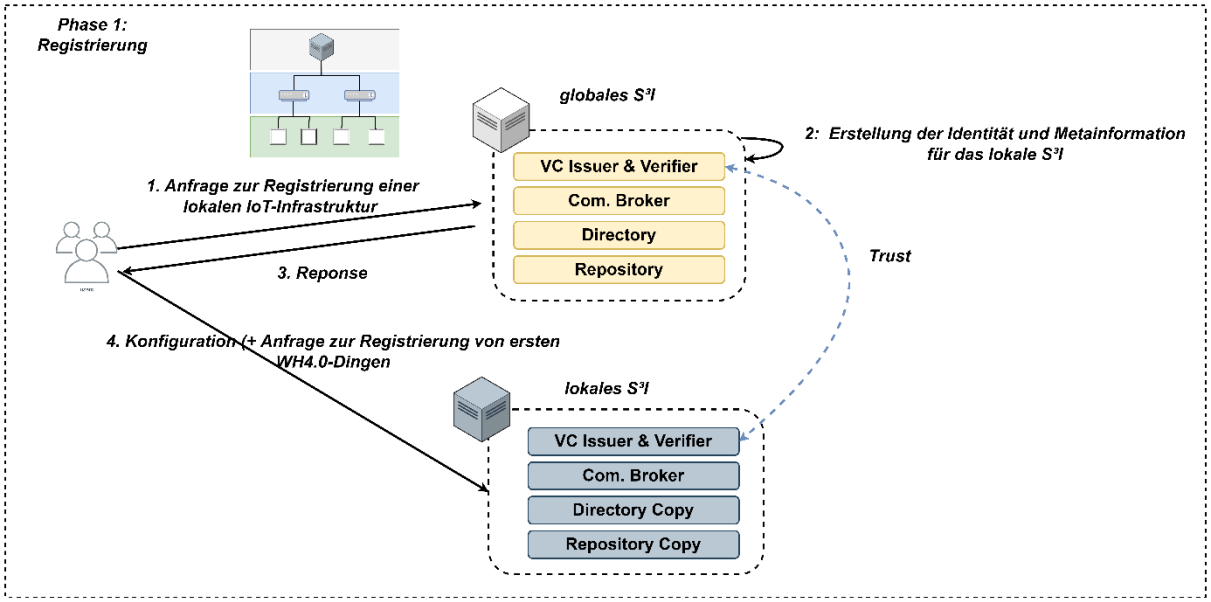

Abbildung 11: Registrierung eines lokalen S³I

5.2.1.2 Kommunikation

Mit einer registrierten lokalen S³I-Infrastruktur lassen sich WH4.0-Dinge anlegen und vernetzen. Dabei lassen sich folgende drei grundsätzliche Kommunikationsszenarien identifizieren:

1) Kommunikation zwischen WH4.0-Dingen **innerhalb derselben** (lokalen oder globalen) S³I-Infrastruktur, z.B. DZ Harvester und Harvester-Fahrer-App tauschen Daten zu Stammabschnitten im Wald aus.
2) Kommunikation zwischen WH4.0-Dingen **verschiedener lokaler** S³I-Infrastrukturen, z.B. DZ Harvester übergibt die Stammabschnitte an DZ Forwarder, der mit anderen separaten lokalen S³I-Infrastruktur verbunden ist.
3) Kommunikation zwischen WH4.0-Dingen **zwischen** einer **lokalen** und der **globalen** S³I-Infrastruktur. Beispielsweise fragt DZ Waldbesitzer den aktuellen Produktionsstatus von DZ Produktionsteam über das globale S³I ab, allerdings ist der DZ aktuell im Wald und mit einer lokalen S³I-Infrastruktur verbunden.

Auf Fall 1) wird im Weiteren nicht eingegangen, weil die Kommunikation hier dem Standardfall von S³I entspricht. Die Fälle 2) und 3) werden in der Prozessbeschreibung in den Varianten Phase 2.1 (siehe Abbildung 12) bzw. Phase 2.2 (siehe Abbildung 13) illustriert.

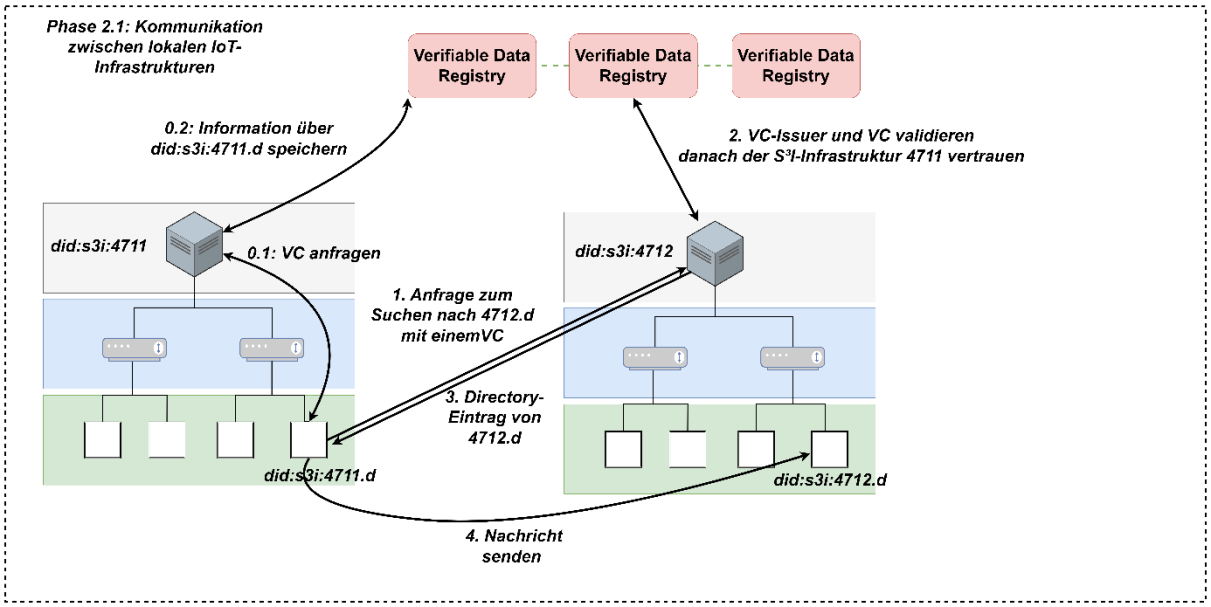

Abbildung 12: Kommunikation der WH4.0-Dinge über zwei verschiedene lokale S³I

Die Kommunikation in Phase 2.1 beginnt mit der Anfrage nach einem VC (Schritt 0.1) von dem WH4.0-Ding (did:s3i:4711.d) bei einer lokalen S³I-Infrastruktur mit Kennung did:s3i:4711. Mit dem VC kann das WH4.0-Ding anschließend seine Identität gegenüber Dritten verifizieren lassen. Der VC-Issuer (von Infrastruktur did:s3i:4711) ist abgesehen von der VC-Ausstellung auch dafür zuständig, Informationen (z.B. public key, Endpunkt für die Authentifizierung …) über das anfragende WH4.0-Ding (did:s3i:4711.d) in einer Verifiable Data Registry (VDR) zu speichern (Schritt 0.2). Technische Basis dieser Registry ist ein dezentralisiertes System, welches als Blockchain oder Distributed Ledger umgesetzt werden kann. Das ausgestellte VC kann dann vom WH4.0-Ding did:s3i:4711.d für weitere Anfragen verwendet werden, auch wenn der angefragte Dienst in einem anderen lokalen S³I ist, siehe Schritt 1 in Abbildung 12. Im Beispiel wird das Directory der lokalen Infrastruktur mit Kennung did:s3i:4712 angefragt. Der VC-Verifier (der Infrastruktur did:s3i:4712) verifiziert das versendete VC sowie dessen VC-Issuer (von Infrastruktur did:s3i:4711) und gibt die angefragten Ressourcen im Directory frei, siehe Schritt 2 und 3.

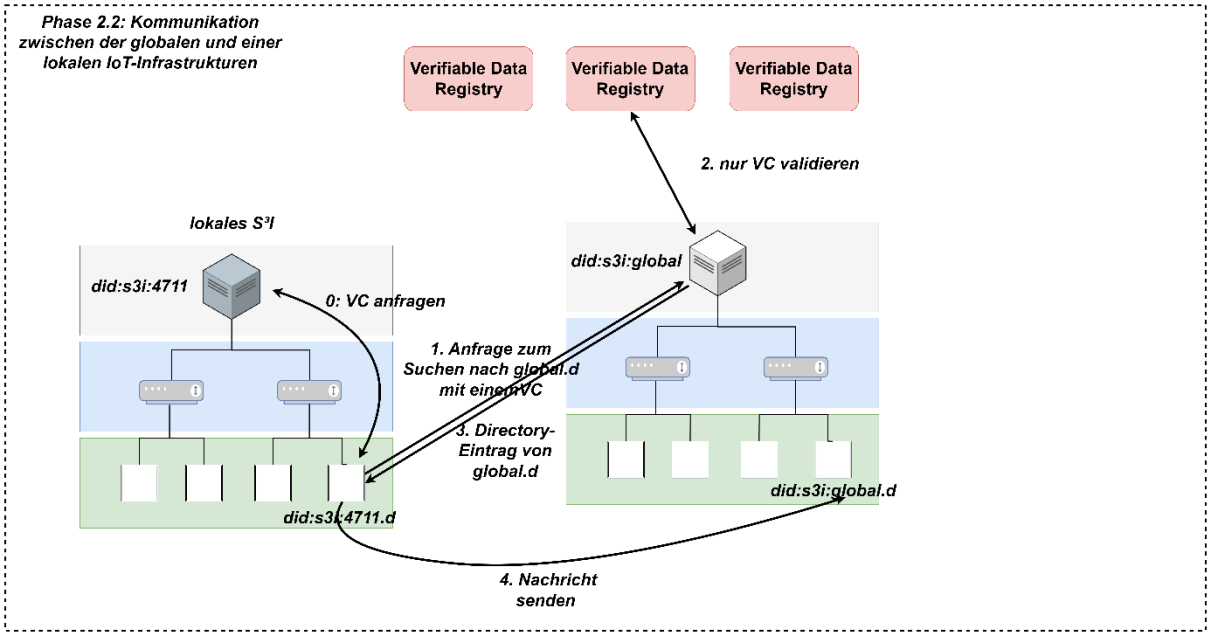

Abbildung 13: Kommunikation der WH4.0-Dinge über ein globales und lokales S³I

Die Kommunikation in Variante Phase 2.2 (siehe Abbildung 13) beschreibt den Kommunikationsfall, in dem das globale S³I involviert ist. Im Vergleich zur Phase 2.1 ist hier keine Verifikation des VC-Issuers mehr notwendig, da die Vertrauenswürdigkeit bereits bei der Registrierung (Phase 1) aufgebaut wird. Abgesehen davon sind die Abläufe identisch.

Eine direkte Kommunikation zwischen den WH4.0-Dingen (Schritt 4 in Phase 2.1 bzw. 2.2) erfolgt dann nach dem Konzept zur Föderierung der Broker, siehe nächster Abschnitt.

5.2.1.3 Direkte Vernetzung über Föderierung der Broker

In Smart Forestry erfolgt der Datenaustausch unmittelbar zwischen den WH4.0-Dingen, auch wenn diese in verschiedenen lokalen oder der globalen IoT-Infrastruktur betrieben werden. Dieser Abschnitt befasst sich mit der direkten Vernetzung zwischen WH4.0-Dingen auf Grundlage eines AMQP-Brokers (RabbitMQ). Dazu werden die drei im vorherigen Abschnitt eingeführten Kommunikationsfälle betrachtet, siehe Abbildung 14. Grundsätzlich wird dazu ein „Federated Link“ zwischen den Broker-Instanzen der verschiedenen S³I-Infrastrukturen etabliert. Dieser Link erlaubt dann die Nachrichten über eine Instanz hinaus weiterzuleiten.

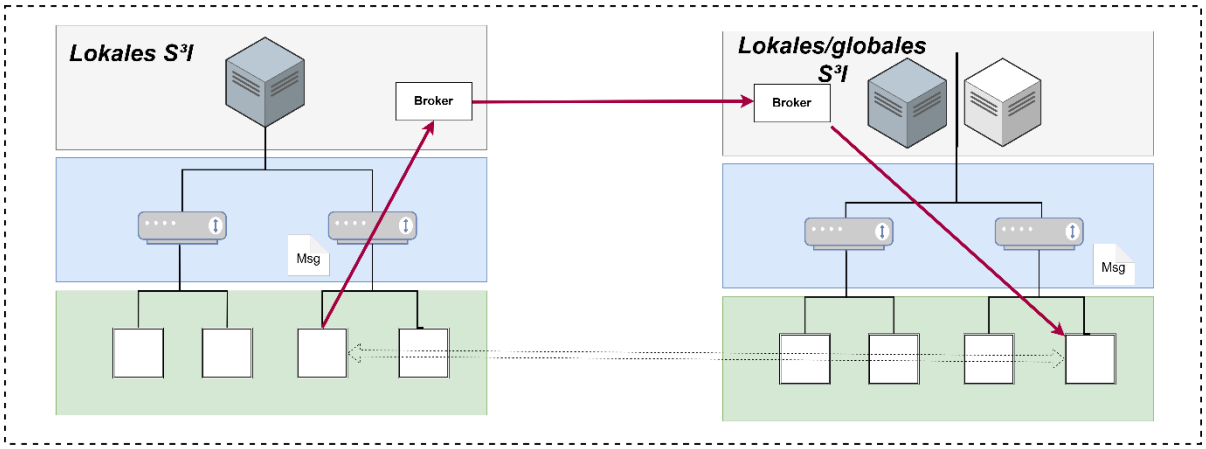

Abbildung 14: Abbildung des Konzepts für föderierte Broker in die drei Kommunikationsfälle

Die technische Umsetzung des S³I-Brokers basiert auf dem Open Source System RabbitMQ, das bereits eine verteilte Umsetzung unterstützt[55]. Die dort konzeptionierte Föderierung erlaubt es, in einem Exchange oder in einer Queue eines Brokers Nachrichten zu empfangen, die in einem Exchange oder in einer Queue eines anderen Brokers veröffentlicht wurden. Föderierte Broker können auf verschiedenen Maschinen/Clustern betrieben werden. Diese können geographisch weit voneinander entfernt sein. Die Verbindung zwischen Brokern kann entweder unidirektional oder bidirektional aufgebaut werden. Diese Verbindung wird „Federation Link“ genannt. Standardmäßig werden Nachrichten nur einmal über einen „Federation Link“ gesendet. In komplexen Topologien (z.B. Stern, Ring und Bus) und abhängig vom konkreten Bedarf an Kommunikationsperformance können Nachrichten mehrfach denselben „Federation Link“ durchfließen, bis sie das Ziel erreichen. Im Fall eines Routings in einer geschlossenen Ringtopologie werden Nachrichten auf den jeweils nächsten Broker weitergeleitet, bis sie das Ziel erreichen. Wenn der Sender die von ihm gesendete Nachricht erhält, wird die Weiterleitung beendet.

Im S³I wird das föderierte Broker Konzept ohne Spezifizierung einer konkreten Topologie implementiert. D.h., es wird ein gewisser Spielraum für Benutzer bereitgestellt, um sich damit individuell für eine Topologie zu entscheiden und diese umzusetzen.

[55] https://www.rabbitmq.com/distributed.html

5.2.2 Realisierung lokaler Infrastrukturen

Die Realisierung lokaler S³I-Infrastrukturen hängt nicht von den Kommunikationsfällen ab, weil diese die Vernetzung auf der S³I-Ebene (somit auch auf der WH4.0-Dinge-Ebene) nicht beeinflussen sollte. Im Rahmen von Smart Forestry lässt sich eine lokale S³I-Infrastruktur ad-hoc-mäßig oder Infrastruktur-mäßig mit einem Router aufbauen, siehe Abbildung 9. Im Folgenden wird auf ad-hoc-basierende lokale S³I-Infrastrukturen eingegangen.

Im Hinblick auf die Anwendung drahtloser Kommunikation erfolgt die forstliche Produktion im Wald typischerweise sehr dynamisch – die Konnektivität der Maschinen kann durch ihre Bewegung abgeschwächt oder verhindert werden. Außerdem wird die Kommunikation unter anderem stark durch die Wetteränderung beeinflusst. Zur Maximierung der Kommunikationsflexibilität von WH4.0-Dingen kommen ad-hoc-Netzwerke zum Einsatz. In solchen Netzwerken können WH4.0-Dinge als dynamische Knoten mit Access Point eingerichtet werden und sich mit den Diensten der lokalen S³I-Infrastruktur ad-hoc-mäßig vernetzen. Die Funkstrecken (eine direkte drahtlose kommunikationstechnische Verbindung zwischen WH4.0-Dingen) lassen sich unabhängig von einer vorkonfigurierten Netzwerkinfrastruktur selbsttätig aufbauen und konfigurieren.

In Smart Forestry wurde auf konzeptueller Ebene untersucht, wie eine WH4.0-mäßige Kommunikation in Ad-hoc-Netzwerken stattfindet bzw. in die gesamte Kommunikationsarchitektur integriert werden kann. Die Auswahl der verwendeten Funktechnologien bzw. Ad-hoc-Protokolle wird dabei weniger berücksichtigt. Hierbei liegt der Fokus hauptsächlich auf der Kommunikation innerhalb eines Ad-hoc-Netzwerks (siehe Kapitel 5.2.2.3).

5.2.2.1 Registrierung

Für den Aufbau eines Ad-hoc-Netzwerks muss Vorkonfiguration getätigt werden, sowohl auf der Seite der Infrastruktur (Identität der ad-hoc-mäßigen, lokalen S³I-Infrastruktur anlegen und Metainformation in die globale S³I-Infrastruktur eintragen) als auch auf der Ebene der WH4.0-Dinge (z.B. Access Point aufsetzen). Die in diesem Abschnitt beschriebene Registrierung bezieht sich auf die Vorkonfiguration des Ad-hoc-Netzwerks auf der Infrastrukturseite. Im WH4.0-Kontext wird ein Ad-hoc-Netzwerk durch Metainformationen spezifiziert. Diese Metainformationen werden bereits bei der Registrierung des Netzwerks angelegt und umfassen u.a.:

- Identität („identifier“)
- Name („name“); im Fall der Kommunikation über WLAN kann „name“ die SSID darstellen
- ggf. das Passwort zur SSID („psk“)
- Endpunkte der vernetzten WH4.0-Dinge („nodes“)

Eine beispielhafte Serialisierung in JSON wäre:

```
{
  "identifier": "ad-hoc:4711",
  "description": "ad-hoc network based local s3i",
  "name": "ad-hoc:4711",
  "psk": "example-password",
  "protocol": "example-protocol",
  "nodes": [
    "ad-hoc:4711://192.168.1.12",
    "ad-hoc:4711://192.168.1.13"
  ]
}
```

Beispiel 2: Metainformation für ad-hoc-mäßige lokale S³I-Infrastruktur

Diese Informationen können dann zum Verbindungsaufbau mit einem Ad-hoc-Netzwerk (somit dann mit den zentralisierten Diensten der S³I-Infrastruktur und WH4.0-Dingen) genutzt werden.

5.2.2.2 Teilnahme an einem Ad-hoc-Netzwerk

Unter der Teilnahme von WH4.0-Dingen an einem Ad-hoc-Netzwerk wird ein kommunikationstechnischer Verbindungsaufbau mit dem Netz verstanden, siehe Abbildung 15. Dafür sind diverse Informationen über das Netzwerk relevant, z.B. einheitliche SSID und einheitliches Passwort für das Ad-hoc-Netzwerk gemäß WiFi IEEE 802.11 ah.

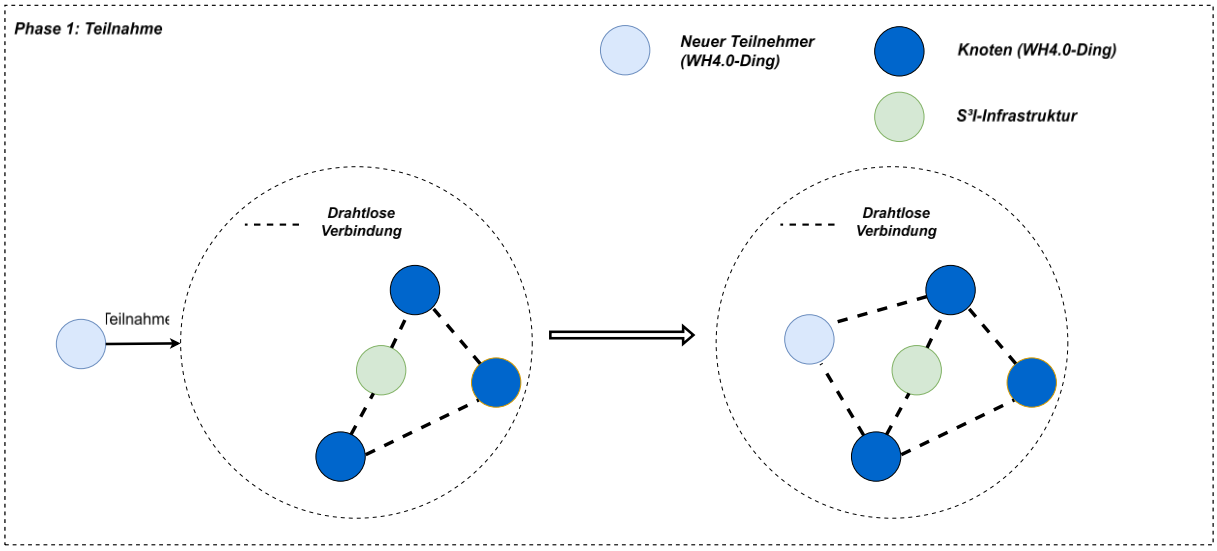

Abbildung 15: Teilnahme an einem bestehenden Ad-hoc-Netzwerk

Zur Vereinfachung des Verbindungsaufbaus können die relevanten Informationen z.B. an der S³I-Box der lokalen S³I-Infrastruktur verfügbar gemacht werden. Nach dem Verbindungsaufbau werden Metainformationen des Teilnehmers (S³I-Directory-Eintrag) im Ad-hoc-Netzwerk verbreitet bzw. im Directory-Dienst der lokalen S³I-Infrastruktur gespeichert.

5.2.2.3 Kommunikation innerhalb eines Ad-hoc-Netzwerks

Die Nutzung eines Ad-hoc-Netzwerks unterstützt WH4.0-Dinge bei einer flexiblen Kommunikation, insbesondere wenn sie keinen Internetzugang haben aber gleichzeitig einen direkten Datenaustausch untereinander ermöglichen wollen.

Wie in Kapitel 2.2.2 vorgestellt, stehen dazu proaktive und reaktive Routing-Protokolle zur Auswahl. Für eine Anwendung im Wald wird empfohlen, ein Tabellen-getriebenes, proaktives Protokoll auszuwählen, z.B. Optimized Link State Routing Protocol (OLSR, siehe Kapitel 2.2.2.1). In dem Fall wird das Routing nur nach Bedarf betrieben, sodass im Netzwerk kein Flooding erfolgen muss. Damit ergibt sich eine effiziente Vernetzung im (Kommunikations-)Ressourcen-beschränkten Wald.

Abbildung 16 zeigt eine schematische Darstellung des Prozesses für einen Nachrichtenversand innerhalb eines Ad-hoc-Netzwerks. Im Allgemeinen lassen sich die Kommunikationsschritte als Entdeckung, Auswahl, Wartung und Repräsentieren (siehe Kapitel 2.2.1) zusammenfassen. Das zu verwendende Ad-hoc-Protokoll muss im Vorfeld festgelegt werden. Jeder Knoten (hier z.B. der Sender und der Empfänger) repräsentiert ein WH4.0-Ding, von dem signierte Nachrichten im S³I-B-Format versendet, weitergeleitet oder empfangen werden. Kommunikationstechnisch wird die AMQP-Schnittstelle des lokalen S³I-Brokers für den Versand der Nachricht aufgerufen und diese auf den unteren OSI-Schichten des Ad-hoc-Netzwerks transportiert. Die Authentifizierung erfolgt „one-way“. D.h. beim Nachrichtempfän-

ger wird die Verifikationsschnittstelle des VC-Verifier aufgerufen, welcher in jeder lokalen S³I-Infrastruktur umgesetzt wird. Der Verifier überprüft die Gültigkeit des VC und bestimmt damit die Autorisierung (Permissions) des Senders.

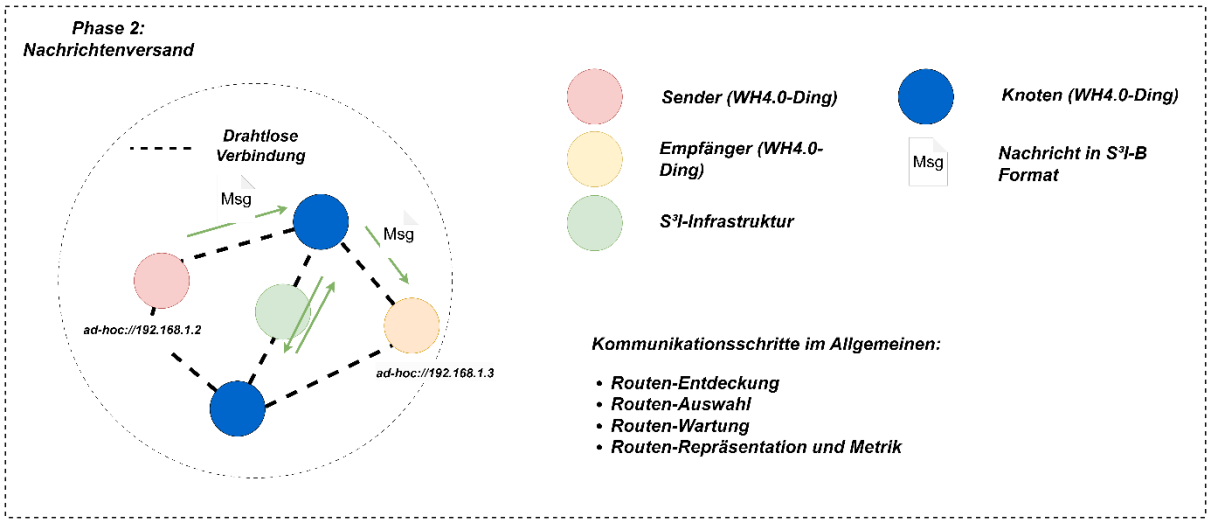

Abbildung 16: Nachrichtenversand innerhalb eines Ad-hoc-Netzwerks

5.3 Informationsmodelle

Um eine einheitliche, verständliche Kommunikation zu betreiben, wurden die Informationsmodelle und eine Modellierungssprache zur Beschreibung der Inhalte der WH4.0-Dinge definiert. In Smart Forestry wird das Metadatenmodell des S³I-Directory genutzt, um ein Informationsmodell eines WH4.0-Dings zu erstellen, siehe Kap. 2.2 in das S³I-Whitepaper[56]. Darüber hinaus beschreibt ForestML 4.0[57] [1] als Modellierungssprache sowohl die Schnittstelle oder Sprache für die Kommunikation untereinander als auch eine formale Struktur der WH4.0-Dinge und der auszutauschenden Daten. Diese werden in Smart Forestry zur Beschreibung der WH4.0-Dinge verwendet bzw. erweitert.

Die Nachrichtenbasierte Kommunikation erfolgt gemäß dem S³I-B-Protokoll. Dieses Protokoll stellt ein konzeptuelles Datenmodell zum Aufbau einer Nachricht dar, aus dem drei grundlegende Typen abgeleitet werden: *UserMessage*, *ServiceMessage* und *AttributeMessage*. Bestehende Informationsmodelle im Wald und Holz (siehe Kap. 2.4) lassen sich als Inhalte direkt in eine S³I-B-Nachricht integrieren.

[56] M. Hoppen 2020, „Konzeption und Einsatz der Smart Systems Service Infrastructure (S³I) zur dezentralen Vernetzung in Wald und Holz 4.0“, https://www.kwh40.de/wp-content/uploads/2020/04/KWH40-Standpunkt-S3I-v2.0.pdf.

[57] M. Hoppen, 2020 „Forest Modelling Language 4.0, Konzeption und Einsatz der Forest Modelling Language 4.0 (fml40) zur Modellierung von Wald und Holz 4.0-Dingen,“ 07 04 2020. https://www.kwh40.de/wp-content/uploads/2020/03/KWH40-Standpunkt-fml40-Version-1.0.pdf.

Kontakt

Smart Forestry war ein Verbundvorhaben der Partner RWTH Aachen (Konsortialführung), Hohenloher Spezial-Maschinenbau GmbH (HSM), Bayerische Staatsforsten AöR (BaySF), IFOS GmbH, ANDREAS STIHL AG & Co. KG, UPM Biochemicals GmbH, Kuratorium für Waldarbeit und Forsttechnik (KWF) e.V. und Landesbetrieb Wald und Holz NRW (Forstliches Bildungszentrum).

Autoren dieses Leitfadens:

- Jiahang Chen, Institut für Mensch-Maschine-Interaktion (MMI) der RWTH Aachen University
- Julia Kemmerer, Bayerische Staatsforsten AöR (BaySF)
- Dr. Dorothea George Mayer, Kuratorium für Waldarbeit und Forsttechnik (KWF) e.V.

Ansprechpartner:
Dr.-Ing. Martin Hoppen
Institut für Mensch-Maschine-Interaktion (MMI) der RWTH Aachen University
hoppen@mmi.rwth-aachen.de
https://www.kwh40.de/smartforestry/

Das Vorhaben wurde gefördert durch das Bundesministerium für Ernährung und Landwirtschaft (BMEL) über seinen Projektträger Fachagentur Nachwachsende Rohstoffe (FNR) e.V. (Förderkennzeichen 2220NR254 A-H). Die 3-jährige Projektlaufzeit war 10/2021 bis 09/2024.

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages