



Projekt LoRaWAN Netzwerk

Zwischenbericht | Call 13 | Projekt ID 3532

Lizenz: CC-BY-SA

(Nicht zutreffendes bitte löschen!)

Inhalt

| | |
|--|----|
| 1. Einleitung..... | 3 |
| 1.1. Hintergrund der Aktivitäten..... | 3 |
| 1.2. Vision & Ziel | 4 |
| 1.3. Der Verein | 4 |
| 2. Arbeitspakete | 5 |
| 2.1. AP2: Planung und Errichtung von Gateways zur Netzabdeckung..... | 5 |
| 2.2. AP3: Entwicklung eines Netzwerktestgeräts & Dokumentation der Netzabdeckung | 9 |
| 2.3. AP4: Errichtung eines Monitoring und Management-Systems für Gateways | 12 |
| 2.4. AP5: Anonymisierung & Veröffentlichung der Daten | 14 |
| 2.5. AP6: Dokumentation | 15 |
| 2.6. AP7: Externkommunikation & Erreichung Sichtbarkeit, Nachhaltigkeit | 16 |
| 2.7. AP8: Entwicklung von drei Use-Cases | 20 |
| 2.8. AP10: Errichtung einer IoT Plattform | 25 |

1. Einleitung

1.1. Hintergrund der Aktivitäten

Im Jahr 2017 haben wir erstmals von LoRaWAN erfahren. Uns hat das Thema sofort angesprochen, weil es sich um einen definierten weltweiten Standard für IoT handelt, der höchste Kompatibilität ermöglicht, zahlreiche Funktionen im Standard umfasst und in Europa auf einer Frequenz betrieben wird, die nicht lizenzpflichtig ist und daher frei genutzt werden darf. Diese Kombination ermöglicht den Aufbau eines vollständig gemanagten Netzes und einer Infrastruktur im Rahmen von nicht gewinnorientierten (non profit) Anwendungen und Organisationen.

Wir glauben, dass IoT eine der nächsten großen Entwicklungen im IKT-Umfeld darstellt bzw. noch verstärkt darstellen wird. Mit LoRaWAN durchbricht man die Schwelle von proprietären Implementierungen und nutzt einen globalen Standard für den Austausch an Daten und Informationen. Ebenso sind unzählige Geräte, Sensoren und Aktoren verfügbar, die zum LoRaWAN-Standard kompatibel sind und daher problemlos genutzt werden können. Ein großer Enabler für IoT ist das gemeinsame Nutzen von Daten - daher ist auch hier Standardisierung wichtig, um aus all den Messdaten ein gemeinsames Ergebnis zu ermöglichen.

Im Jahr 2017 haben sich auch andere Technologien (und deren Interessenvertretungen) um einen Platz in der IoT-Welt bemüht, insbesondere im Bereich LPWAN (Low Power Wide Area Networks). Diese sind neben LoRaWAN beispielsweise SigFox oder NB-IoT. Wir haben diese Technologien hinterfragt und sind zu dem Ergebnis gekommen, dass LoRaWAN unser Weg ist. Der Standard ist offen verfügbar und klar definiert, es gibt mehrere Implementierungen für den LoRaWAN-Stack - auch in der Open Source-Welt. SigFox ist beispielsweise nicht als offener Standard publiziert, die Netze sind zentral verwaltet und die Nutzung teilweise unter einer Lizenz vergeben. Für NB-IoT (ebenso wie LTE-M) sind Frequenzen der Mobilfunkanbieter zu nutzen, wodurch die Errichtung eines freien und offenen Netzes nicht möglich ist.

Rückblickend - nach etwas mehr als zwei Jahren Erfahrung mit dem Thema - haben wir mit LoRaWAN die richtige Entscheidung getroffen: mittlerweile haben wir ein Netz errichtet, das den Großraum Wien im Freien sehr gut abdeckt. Es sind zahlreiche Anwendungen - teilweise mit unserer Hilfe und Unterstützung - implementiert worden und das Ecosystem hat sich bewährt. Auch im Enterprise & Industrie-Umfeld ist erkennbar, dass sich LoRaWAN und NB-IoT/LTE-M als de-facto Standards in vielen Ländern Europas etabliert haben. In der Schweiz hat Swisscom ein kommerzielles LoRaWAN-Netz errichtet, das schweizweit eine Abdeckung von 97% der Bevölkerung im Außenbereich

(https://documents.swisscom.com/product/filestore/lib/84eb9c67-84fa-4e05-b5b0-c54c4baeeca7/fs_lpn-de.pdf) bereits heute ermöglicht. In Holland hat KPN ein LoRaWAN-Netz errichtet, das landesweit angeboten wird. Auch in Österreich gibt es einen kommerziellen Anbieter, der gerade ein kommerzielles LoRaWAN-Netz errichtet.

Wir nutzen hier also keine Nischen-Technologie, sondern errichten ein freies und offenes Netz, das kompatibel zu einem de-facto-Standard der kommerziellen Welt ist.

Es gibt eine weltweite Initiative, von Holland ausgehen, die ein globales freies und offenes Netzwerk auf Basis LoRaWAN koordiniert: The Things Network (<https://www.thethingsnetwork.org>). Wir haben beschlossen, unsere Gateways an das Netz von The Things Network (TTN) zu koppeln. Dadurch sind wir Teil einer weltweiten Community und unsere Sensoren und Anwendungen funktionieren nicht nur in unserer geografischen Region, sondern können im gesamten Netz von TTN genutzt werden. Dieses Netz ist aktuell mit weltweit 8.946 Gateways in 141 Ländern verfügbar (Stand September 2019).

Es ist spannend, dass nun unsere Sensordaten nicht nur von unseren Gateways empfangen werden, sondern oft auch von Partnernetzen in Bratislava oder Brünn. Damit ergänzen sich die Netze wunderbar und es gibt keine harten Übergänge zwischen Regionen. Es ist auch toll, zB. im Urlaub diese Technologie in Frankreich genauso nutzen zu können wie in Belgien oder Portugal. Aufgrund des freien und offenen Charakters des Netzes funktioniert dies ohne spezielle Konfiguration und natürlich ohne Roamingkosten oder sonstige Aufwände. Einfach den Sensor einpacken und zB. in ganz Europa kostenfrei nutzen!

1.2. Vision & Ziel

Wir glauben, dass IoT eine Technologie bereitstellt, mit der Anwendungen ermöglicht werden, die in Zukunft von jedermann frei und offen genutzt werden sollen. Wir möchten eine Infrastruktur schaffen, mit der wir den Zugang zu und die Nutzung dieser Technologie kostenfrei ermöglichen.

Wenn in einigen Jahren der Bereich IoT auch das Privatkundensegment erreicht, soll die Nutzung der Vorteile dieser Möglichkeiten nicht an einen kommerziellen Vertrag mit einem Netzbetreiber gebunden sein. Es muss frei und offen für alle funktionieren.

1.3. Der Verein

Innerhalb der ersten Monate, in denen wir uns mit LoRaWAN beschäftigt haben, wurde uns klar, dass die Gruppe an Interessenten so groß ist, dass wir uns über einen Verein organisieren. Im Sommer 2017 haben wir diesen dann gegründet. Für den Verein haben wir vier Tätigkeitsbereiche definiert:

1. Sensoren: wir haben eigene Sensoren für unsere Anwendungen entwickelt, testen Sensoren, die am Markt verfügbar sind und helfen - zB. im Zuge von Workshops - bei der Erstellung und Konfiguration von Sensoren sowie der Einbindung ins LoRaWAN-Netzwerk; Publikationen als Open Source wurden mehrfach durchgeführt.
2. Netzwerk: im Bereich Infrastruktur errichten wir Gateways, um die Reichweite und Netzabdeckung für LoRaWAN zu verbessern. Auch das Management, der Betrieb der Gateways und Tools für das Deployment gehören zu diesem Handlungsfeld.
3. Plattform: um die Sensordaten auswerten zu können, aber auch um die Funktion des LoRaWAN-Netzes nachzuvollziehen, betreiben wir eine eigene Serverplattform.
4. Community: wir organisieren zahlreiche Events zum Thema LoRaWAN & IoT: Community Meetings, die für alle zugänglich sind, finden etwa alle 2 Monate statt. Dazwischen gibt es Arbeitsgruppen, die sich auf bestimmte Themen fokussieren, zB. ein Gateway-Workshop im Frühjahr 2019, bei dem wir gemeinsam über die Funktion

von LoRaWAN Gateways berichtet haben und auch etliche Gateways für den Netzausbau gemeinsam konfiguriert haben.

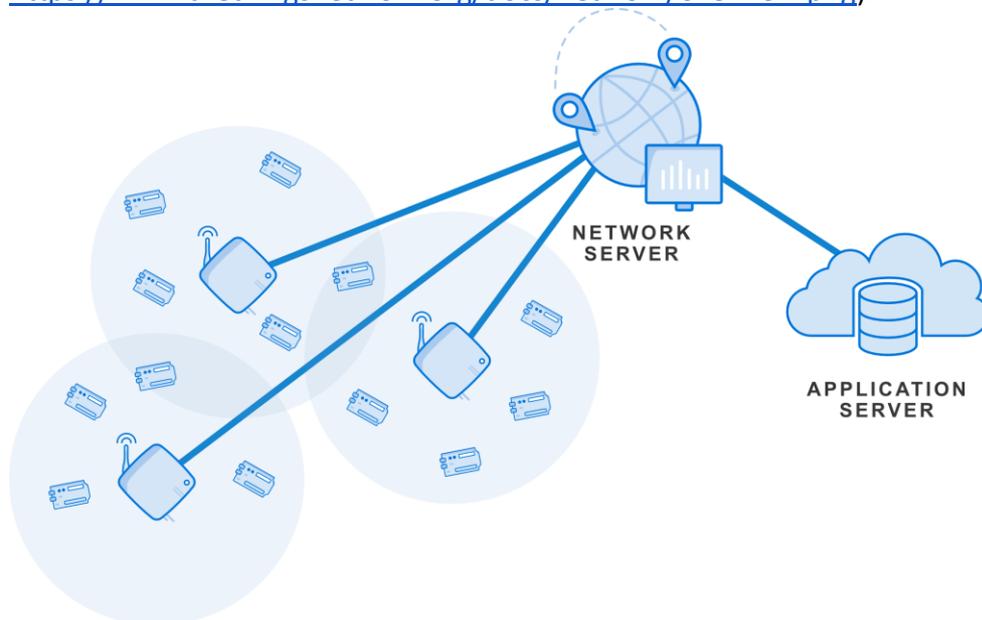
Obwohl wir Mitglieder beim Verein aufnehmen, ist die Nutzung der Infrastruktur auch ohne Vereinsmitgliedschaft möglich. Einfach anmelden und das Netz nutzen. Die Vereinsmitgliedschaft ist für Personen, die aktiv die Richtung des Vereins gestalten möchten, also in der Organisation und Administration mitwirken möchten. Mit der Mitgliedschaft geht auch die Stimmberechtigung bei der Hauptversammlung einher.

Die Mitarbeit im Verein erfolgt ohne Ausnahme ehrenamtlich und in der persönlichen Freizeit. Wir sind sehr stolz auf das Erreichte, vor allem im Hinblick auf die knappen zeitlichen Ressourcen der Mitstreiter/innen.

2. Arbeitspakete

2.1. AP2: Planung und Errichtung von Gateways zur Netzabdeckung

Unsere Initiative hat sich geformt, um IoT Devices über den LoRaWAN-Standard besser zu verstehen und zu betreiben. Das setzt ein Netzwerk voraus. Der Aufbau eines LoRaWAN-Netzes und die Elemente und Aufgaben sind definiert (Quelle: <https://www.thethingsnetwork.org/docs/network/overview.png>):



Neben den Softwaremodulen "Network Server" und "Application Server" sind vor allem die Gateways ein sehr aufwändiger Teil, mit dem wir uns in diesem Arbeitspaket beschäftigen:

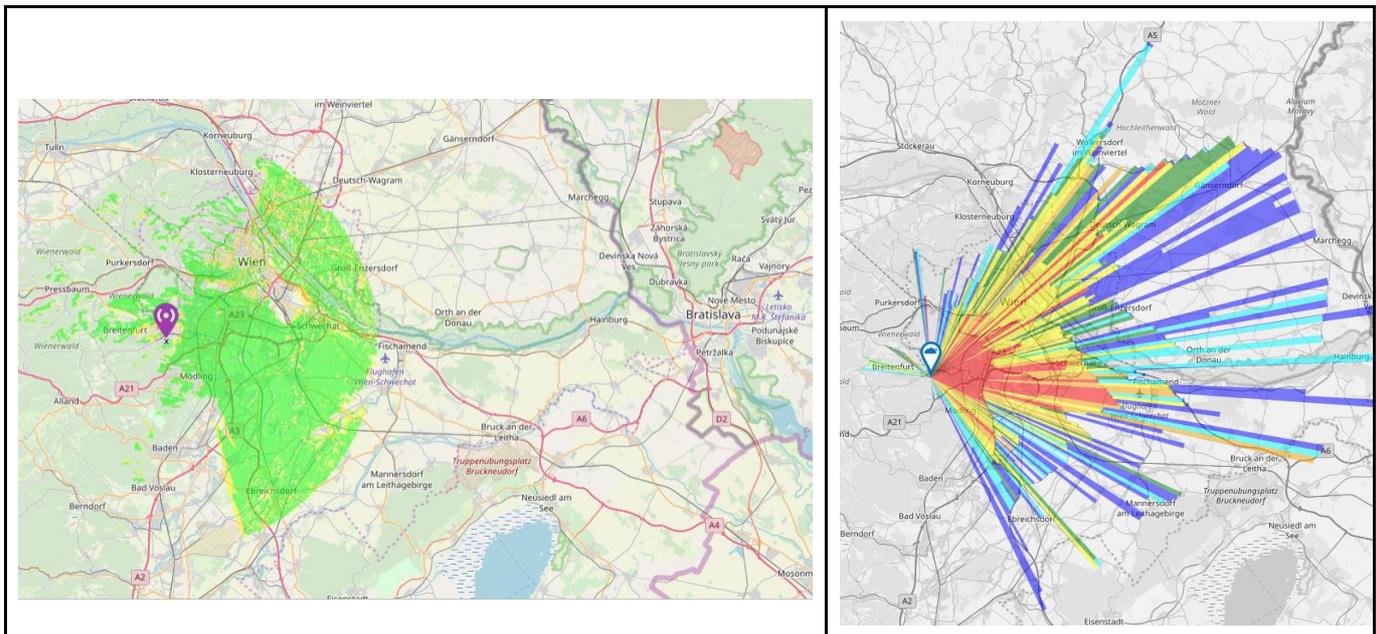
2.1.1. Planung des Netzwerks

Vor der Förderung durch Netidee haben wir einzelne Gateways errichtet, wodurch uns die Reichweiten der Funkabdeckung und Hauptmerkmale, um Standorte für die Installation zu finden, schon etwas bekannt waren.

Wir haben Kooperationen mit den Österreichischen Funkamateuren (<https://www.oevsv.at>) und dem Verein Funkfeuer Wien (<https://www.funkfeuer.at>) abgeschlossen und können somit deren Standorte mit nutzen. Im Gegensatz werden wir auf Standorten, die wir neu errichten, auch Projekte vom ÖVSV und Funkfeuer mit berücksichtigen.

Für die Funkplanung haben wir das Online Programm "Radio Mobile" genutzt, das eine Berechnung auf einer ähnlichen Frequenz (911 MHz statt 868 MHz) sehr professionell ermöglicht und auch über die Geodaten (Höhenprofile), Flächennutzung (Wald, Stadt, durchschnittliche Gebäudehöhen, etc.) verfügt. Die Ergebnisse können exportiert werden bzw. als PDF dargestellt.

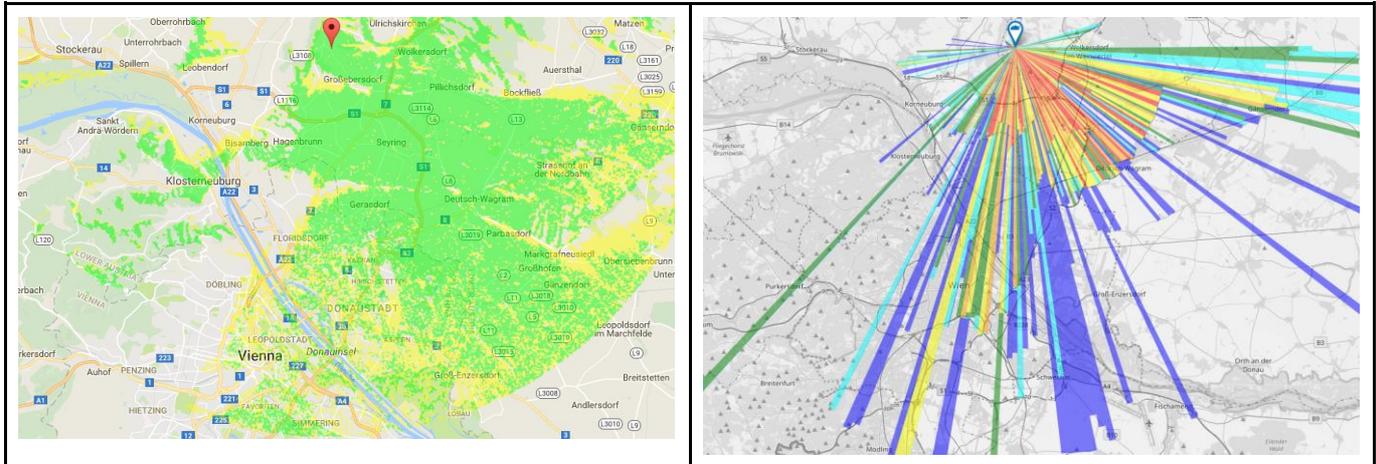
Hier ein Beispiel vom Standort "Franz Ferdinand Hütte" bei Perchtoldsdorf: links die Berechnung der Reichweite (max. 25km), recht eine Messung ca. 1 Jahr nach Betrieb eines Gateways an dem Standort:



Die Gegenüberstellung zeigt, dass vor allem die Richtung der Ausbreitung korrekt berechnet wurde. Die Reichweite ist bei LoRaWAN schwer zu bewerten: die weltweit längste Übertragung eines Signals mit üblichem Equipment liegt bei etwa 800km bei freier Sicht. Es hängt also maßgeblich von Objekten in der Funkstrecke ab, die das Signal dämpfen. Unsere Berechnung im Beispiel oben endet nach 25km. Übertragungen darüber hinaus sind möglich, wie die Messung beweist.

Hier ein weiteres Beispiel zur Reichweite unseres Gateways in Mannhartsbrunn. Auch hier stimmt die Richtung. Die Reichweite ist schwer zu bewerten, weil wir von Messungen im Weinviertel aktuell weniger Testpunkte haben und die Stadt Wien mit den Gebäuden starke

Dämpfung hinzufügt. Die Versorgung im Norden Wiens und Teilen des Weinviertels ist durch Mannhartsbrunn jedoch erfolgreich gegeben:

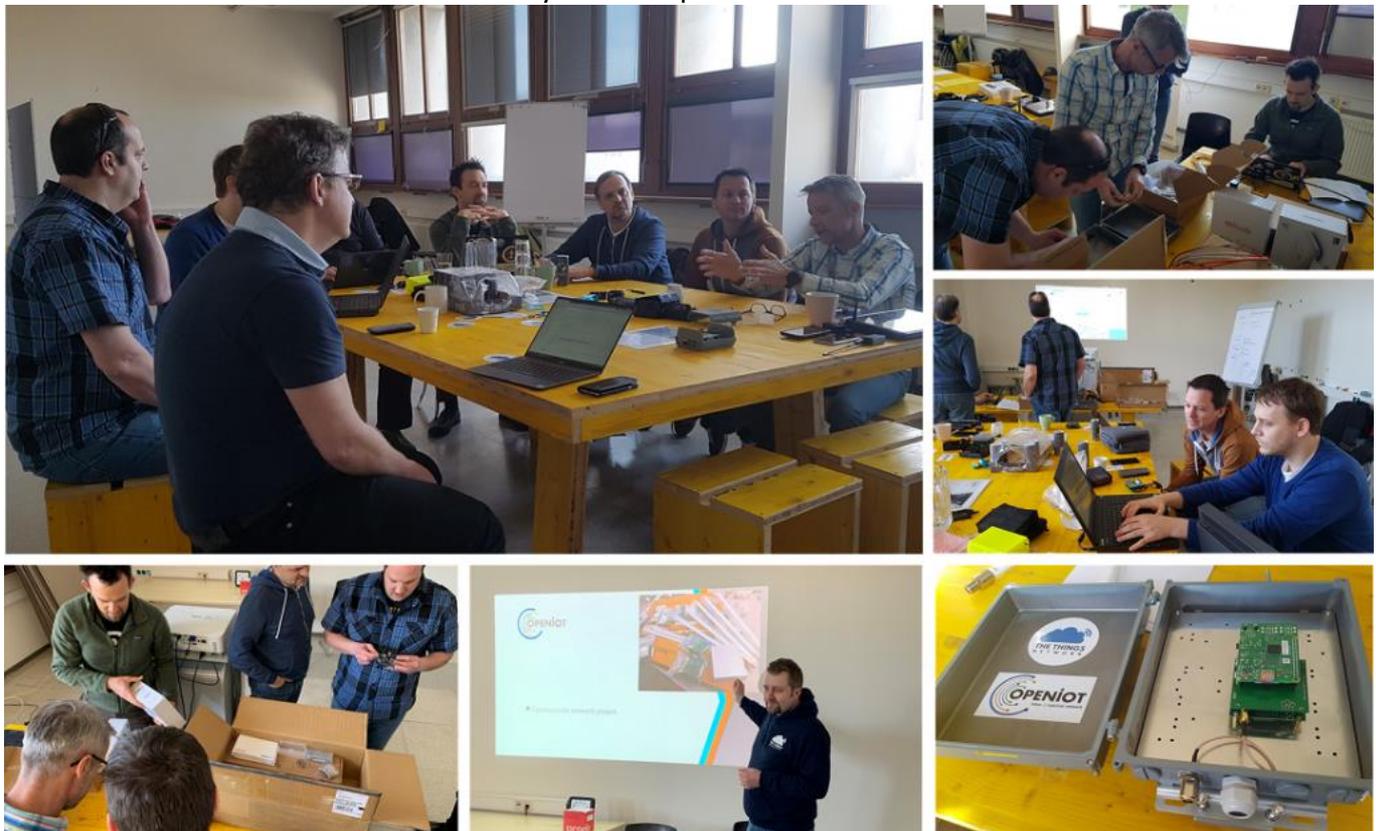


2.1.2. Errichtung des Netzwerks

Nachdem die zentrale Serverseite vorbereitet war, haben wir uns daran gemacht, zahlreiche Gateways auszurollen.

Um die Fertigung der Gateways rascher durchzuführen, haben wir einen Workshop im Februar 2019 durchgeführt und Mithelfer eingeladen. Dort haben wir auch allgemein über die Technologie berichtet und dann mehrere Gateways installiert, zusammengebaut und Helfern übergeben, die diese in den nächsten Wochen in Betrieb genommen haben.

Hier ein Bild mit Eindrücken vom Gateway Workshop:

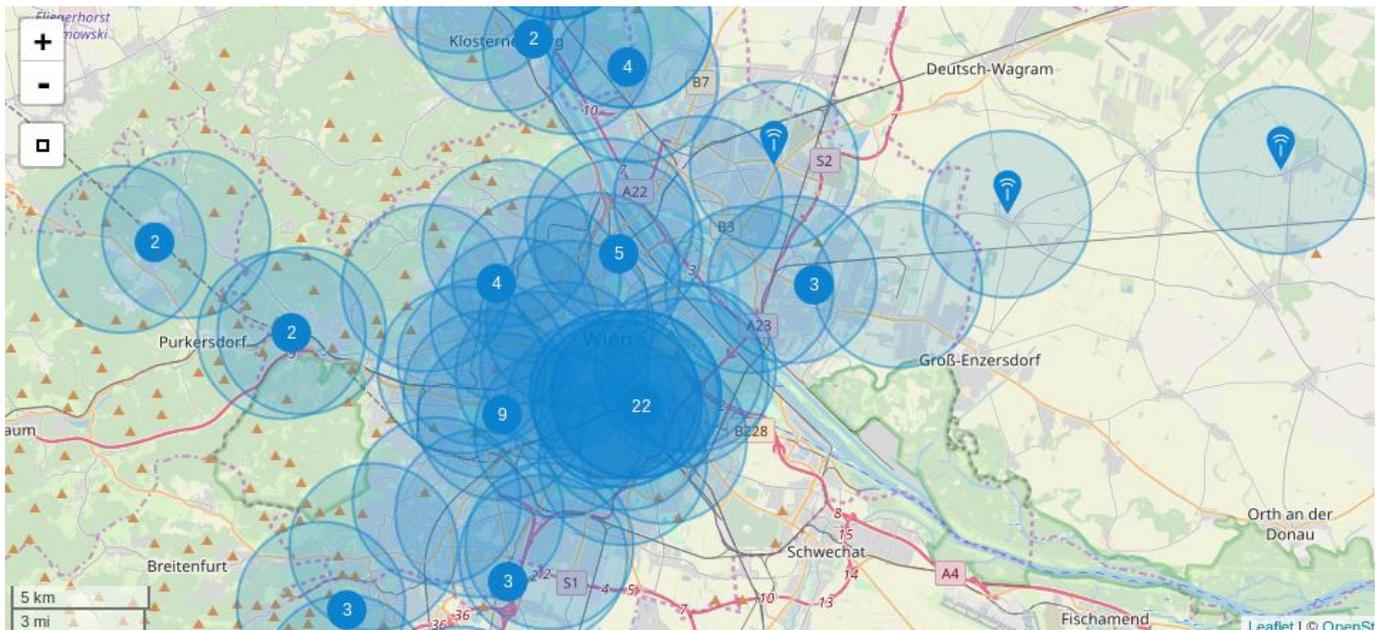


Liste der Gateways, die durch OpenIoT oder mit Unterstützung von OpenIoT errichtet wurden:

| Name des Gateways | Standort | EUI / ID |
|--------------------------|--|----------------------|
| OpenIoT Stefan | Wien, Nähe Belvedere | eui-b827ebfffe061eed |
| OpenIoT Peter | Bisamberg | eui-58a0cbfffe800413 |
| OpenIoT Hadersdorf 1 | Wien, Hadersdorf/Hütteldorf | eui-b827ebfffe09813e |
| OpenIoT Mannhartsbrunn | Mannhartsbrunn | eui-b827ebfffe4a742c |
| OpenIoT SanktElisabeth 1 | Wien, Nähe Schwarzenbergplatz | eui-b827ebfffea52cab |
| OpenIoT OE1NSU | Wien, Rosenhügel | eui-b827ebfffe82bfc7 |
| OpenIoT Peter Jordan | Wien, Nussberg | eui-b827ebfffe95d88e |
| OpenIoT OE1RBU | Wien, Schafberg | eui-b827ebfffeab79e2 |
| OpenIoT lax2 | Wien, Nähe Hauptbahnhof | eui-b827ebfffed93660 |
| OpenIoT Gießhübl | Gießhübl | eui-b827ebfffef21d5f |
| OpenIoT Prottes | Prottes bei Gänserndorf | eui-b827ebfffef5fdfd |
| OpenIoT FFH | Franz Ferdinand Hütte, Perchtoldsdf | eui-b827ebfffeb1ca76 |
| OpenIoT Bisamberg | Wien Strebersdorf | eui-fcc23dfffe0a8b47 |
| OpenIoT Brenner | Wien Simmering | eui-fcc23dfffe0dbc1f |

Durch unsere Aktivitäten konnten wir andere Mitstreiter und auch Organisationen (Bosch, ÖBB, ua.) dazu bewegen Gateways zu errichten und die Netzabdeckung eines gemeinsamen offenen Netzes zu unterstützen.

Bei The Things Network werden mittlerweile 63 Gateways zur Vienna Community gezählt:



(Quelle: <https://www.thethingsnetwork.org/community/vienna/>)

2.1.3. Status des Arbeitspakets

Die Umgebung zur Planung von Standorten bzw. zur Erkennung des Bedarfs ist verfügbar und wird laufend genutzt. Das Arbeitspaket ist inhaltlich abgeschlossen. Es werden weiterhin Standorte dem Netz hinzugefügt.

[100%]

Wie an der Tabelle ersichtlich ist, wurden in den letzten Monaten viele Standorte erschlossen. Der Ausbau des Netzes läuft weiterhin. [50%]

2.2. AP3: Entwicklung eines Netzwerktestgeräts & Dokumentation der Netzabdeckung

Im Zuge der Errichtung des LoRaWAN-Netzwerks möchten wir natürlich die Funktion prüfen und besser verstehen, wie gut Erweiterungen am Netzwerk der Funkabdeckung dienlich sind.

Die Idee war, auf Basis eines Arduino Uno-Geräts (Mikroprozessor) mit einem LoRa+GPS-Aufsteckmodul (Dragino LoRa-GPS-Shield) einen GPS-Tracker zu entwickeln, mit dem wir Informationen zur Netzabdeckung generieren.

Seit einigen Jahren gibt es im Internet eine Webseite, die Informationen zur Abdeckung von LoRaWAN-Netzes im Rahmen von The Things Network grafisch abbildet:

<https://ttnmapper.org/>. Dort wird auch eine Heatmap errechnet, die eine bessere Darstellung ermöglicht.

2.2.1. Entwicklung eines Netzwerktestgeräts

Wie erwähnt haben wir auf Basis

- Arduino Uno (<https://store.arduino.cc/arduino-uno-rev3>) und
- Dragino LoRa GPS Shield (<https://www.tindie.com/products/edwin/loragps-shield-for-arduino/>)

Software entwickelt, die zyklisch Positionsdaten sendet, sobald ein GPS Signal verfügbar ist. In dem LoRaWAN-Paket sind auch Informationen zu den Gateways enthalten, die das Paket empfangen haben. Daraus kann die Reichweite festgestellt werden. Die Daten helfen auch bei der Netzwerkplanung, weil darüber die Reichweite der einzelnen Gateways bekannt ist, inkl. der Auswirkungen, falls es zu einem Ausfall kommt.

Die Software haben wir als Open Source auf Github veröffentlicht:

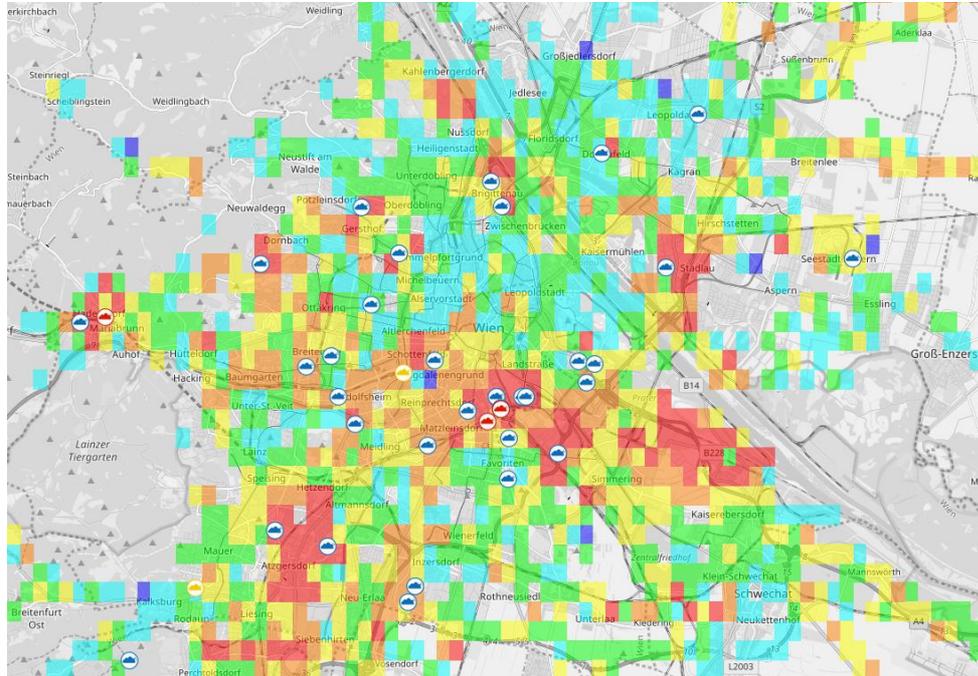
<https://github.com/OpenlotNetwork/LoRa-gpstrack>

Der Software liegt auch eine kleine Dokumentation für den Nachbau des Sensors und die Konfiguration der Einstellungen bei.

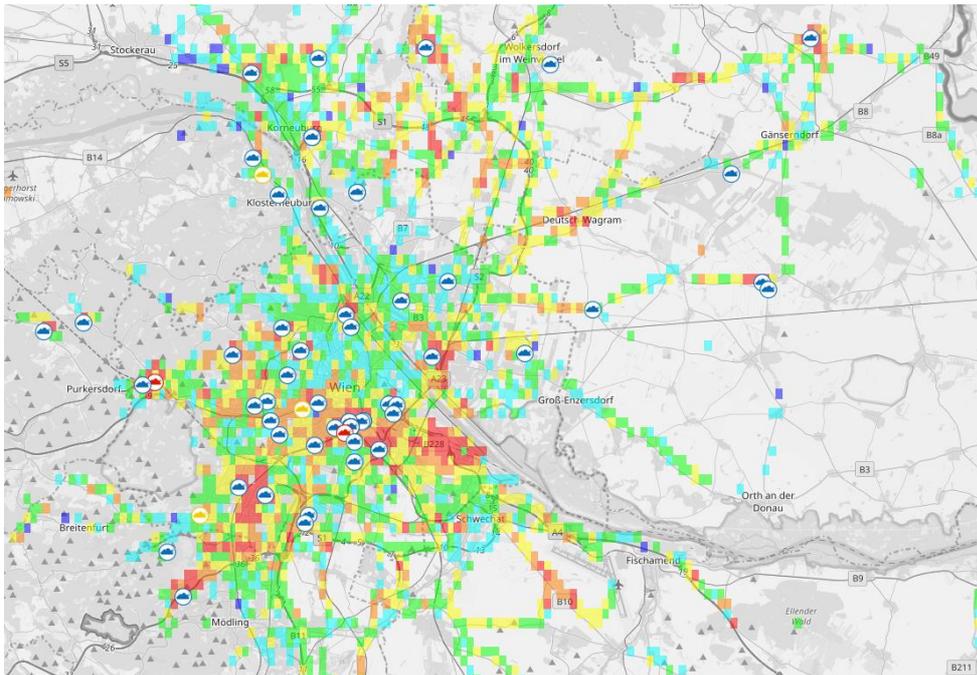
Das Netzwerktestgerät haben wir mehrfach gebaut und teilweise in unsere KFZ integriert. Bei jeder Fahrt wird mit der Zündung das Testgerät aktiviert und während der Fahrt die Reichweite gemessen. Das passiert ohne Aufwand für den Fahrer/die Fahrerin. Ein Nebeneffekt ist, dass die Straßen besser gemessen werden, als die Bereiche dazwischen. Das ist bei der Interpretation der Karten wichtig: die Karten zeigen nur Bereiche in denen gemessen wurden.

2.2.2. Dokumentation der Netzabdeckung

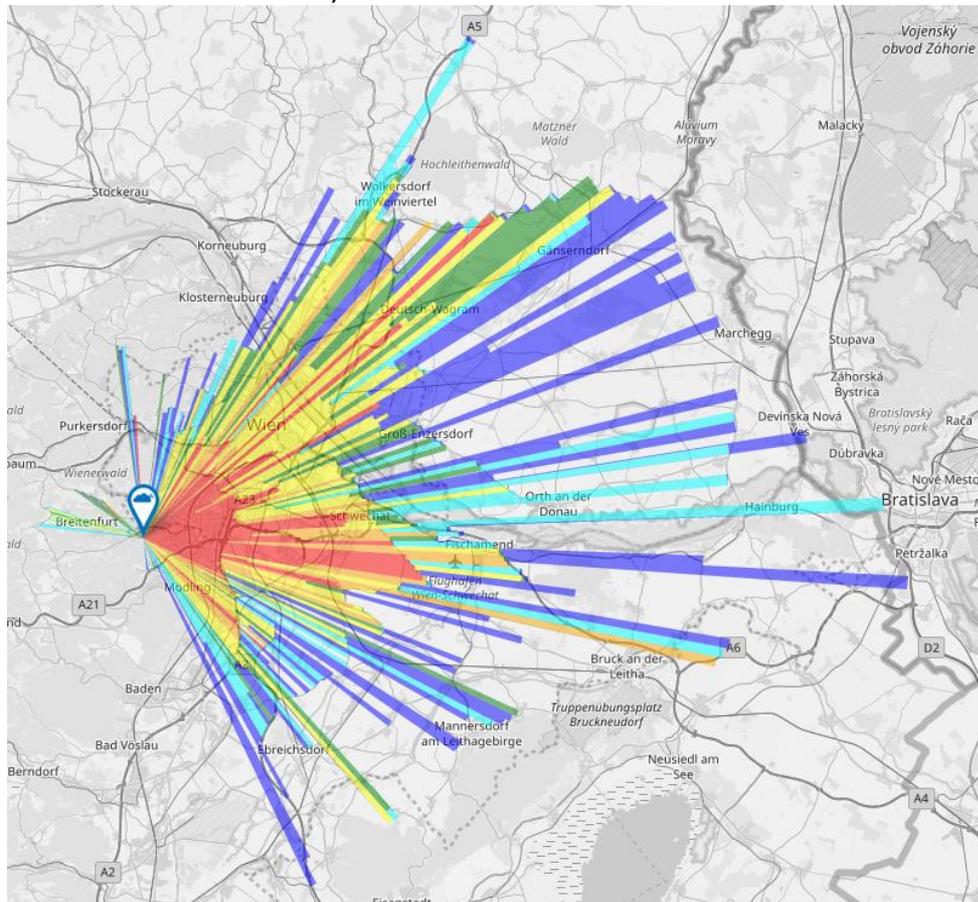
Auf dieser Heatmap, die mit dem Netzwerktestgerät erzeugt wurde, sieht man die Netzwerkabdeckung zum 7. September 2019 im Wiener Bereich:



Diese Karte zeigt die Abdeckung im umliegenden Bereich:



Hier ein Beispiel für die Abdeckung/Reichweite eines einzelnen Gateways (Franz Ferdinand Hütte bei Perchtoldsdorf):



2.2.3. Status des Arbeitspakets

Das Netzwerktestgerät ist erstellt und mehrfach im Einsatz. [100%]

Die Umgebung für die Dokumentation ist vorbereitet und die Messgeräte sind eingebunden. Das System erweitert die Reichweitenkarte automatisch. Daten werden alle 24h aktualisiert. [100%]

2.3. AP4: Errichtung eines Monitoring und Management-Systems für Gateways

Wir nutzen für den Aufbau und Betrieb des LoRaWAN-Netzwerks zwei Produkte:

1. der größte Teil unserer Gateways basiert auf Raspberry Pi (Modell 3B und 3B+ an neueren Standorten). Diese werden mit einem ic880a-LoRaWAN-Concentrator-Board (<https://www.wireless-solutions.de/products/long-range-radio/ic880a.html>) versehen (Aufsteckmodul) und werden über entsprechende Open-Source-Software zu Empfangs- & Sende-Gateway im LoRaWAN-Netzwerk.
2. an einzelnen Standorten testen wir Lorix One-Geräte des Herstellers Wifix. Diese Geräte basieren auf Yocto-Linux (<https://www.yoctoproject.org/>), einer Open Source Linux-Implementierung für Embedded Devices.

Nachdem diese Geräte dezentral - an teils sehr exponierten Standorten - montiert werden (um beste Funkabdeckung und kurze Antennenleitungen zu ermöglichen), benötigen wir eine Lösung für das Monitoring und Management unserer Umgebung. Dies ist auch erforderlich, um unseren Qualitätsanspruch an hohe Verfügbarkeit des Netzes zu erreichen.

Wir haben folgende Bereiche identifiziert, die im Bezug auf Monitoring und Management vordergründig relevant sind:

- Monitoring:
 - Verfügbarkeit des Gateways (Gerät, Hardware, Netzwerkanbindung)
 - frühzeitiges Erkennen auftretender Probleme (Temperatur) und
 - bestmögliche Überwachung der Funktion (siehe AP5: Anonymisierung und Veröffentlichung der Daten).
- Management:
 - Konfigurationsmanagement und
 - Update-/Software-/Patch-Management

2.3.1. Monitoring

Um die Anforderungen an den Bereich Monitoring zu erfüllen, setzen wir die Open Source Software Zabbix (<https://www.zabbix.com/>) ein:

Durch Zabbix ist es möglich, Geräte (in unserem Fall: Linux Hosts) von der Ferne zu überwachen, als auch einen Agent zu installieren, der Parameter vom Betriebssystem oder der Hardware übermittelt. Ebenso ist eine intelligente Alarmierung möglich, die uns hilft, bei Störungen die Ursache rascher zu identifizieren und die Email-Flut zu reduzieren. Aufgrund unserer Kooperationen mit den Österreichischen Funkamateuren (<https://www.oevsv.at>)

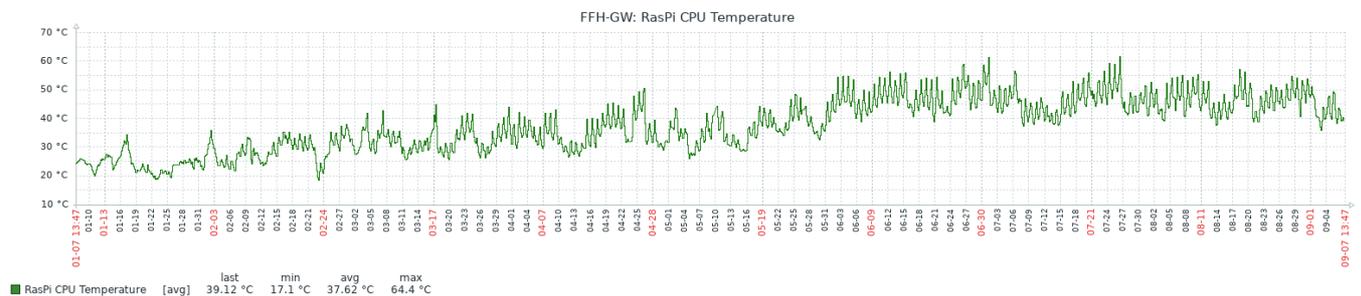
und dem Verein Funkfeuer Wien (<https://www.funkfeuer.at>) sind einige unserer Gateways mittels (Richt)funk angebunden und daher zB. bei starkem Schneefall manchmal beeinträchtigt. Die Policies in Zabbix erlauben uns, solche Zusammenhänge zu erkennen und Hinweise bei der Alarmierung mitzuliefern.

Mit Zabbix überwachen wir somit:

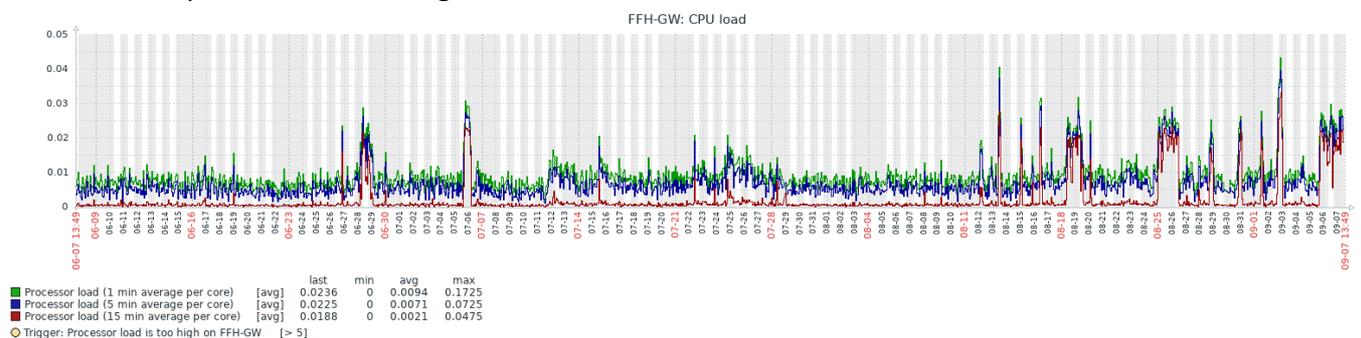
- die Verfügbarkeit der Gateways, inkl. Alarmierungen bei Ausfällen
- die Qualität der Netzwerkanbindung (Erreichbarkeit, Paketverlust, Aufteilung der Protokolle in TCP, UDP und ICMP)
- Auslastung des Betriebssystems (Load, CPU Last, CPU interrupts, Netzwerkverkehr bit/s, Anzahl laufender Prozesse, Auslastung der Festplatte)
- Temperatur des Systems

Die Funktion zur Messung der Temperatur haben wir speziell implementiert, da wir mögliche Fehlfunktionen mit der Witterung in Verbindung bringen möchten. Viele Gateways sind - wie erwähnt - an sehr exponierten Standorten platziert. Raspberry Pi unterstützt das Auslesen der CPU Core Temperatur, wodurch wir diesen vorhandenen Sensor nun implementiert haben.

Hier ein Beispiel für die CPU-Temperatur (seit Beginn unserer Messung vor 8 Monaten) des Gateways auf der Franz-Ferdinand-Hütte bei Perchtoldsdorf; der Temperaturanstieg im Sommer ist klar erkennbar):



Anbei ein Beispiel für die Messung der CPU Last in den letzten 3 Monaten:



2.3.2. Management

Primär haben wir Handlungsbedarf beim Konfigurationsmanagement, sowie beim Pflegen von Updates und Patches.

Zur Umsetzung dieses Managements haben wir uns für die Open Source Software Ansible (<https://www.ansible.com/>) entschieden. Über Ansible pflegen wir unser Inventory und stellen sicher, dass die Software-Stände der Gateways abgestimmt sind. Auch

Konfigurationsänderungen sind über Ansible möglich. Ansible erfordert keinen Client am Gateway und ist daher

Um unseren Mitgliedern das Management in Zukunft noch einfacher zugänglich zu machen, installieren wir in Kürze awx (die Open Source Version des RedHat Ansible Tower). awx (<https://github.com/ansible/awx>) stellt ein Webinterface zu Verfügung, über das wir Ansible Jobs erstellen, pflegen und verwalten können.

Für die Zukunft überlegen wir, vollständig bei der Installation von neuen Gateways auf Ansible zu setzen. Damit sollte ein aufwändiger Schritt bei der Erweiterung der Netze wesentlich vereinfacht werden, während Ansible die Standardisierung der Umgebung sicherstellt.

2.3.3. Status des Arbeitspakets

Die Integration von Zabbix ist abgeschlossen. Die Gateways sind bereits integriert und werden darüber betrieben. [100%]

Die Integration von Ansible ist noch nicht auf allen Gateways abgeschlossen. Für die Zukunft möchten wir jedoch auch awx als grafische Oberfläche nutzen. An der Konfiguration wird aktuell gearbeitet. [60%]

2.4. AP5: Anonymisierung & Veröffentlichung der Daten

Wie beschrieben betreiben wir ein LoRaWAN Netzwerk in Wien. Dazu haben wir zahlreiche Gateways errichtet. Der LoRaWAN-Standard schreibt für Österreich (EU) vor, dass mindestens 3 Kanäle zur Übertragung bereitstehen bzw. verfügbar sein müssen (868.1, 868.3 & 868.5 MHz). Dazu gibt es Empfehlungen, welche weiteren Kanäle (bis zu 8 sind üblich) für die Kommunikation genutzt werden.

Unsere Gateways empfangen somit nicht nur Pakete die an unser Netz gerichtet sind, sondern auch Pakete aus anderen Netzen. Die Daten können zwar nicht entschlüsselt werden, aber die Metadaten (genutzte Frequenz, Dauer, Spreading Factor, etc.) können wir auswerten.

2.4.1. Anonymisierung

Daten werden in einem LoRaWAN-Netzwerk immer (!) verschlüsselt übertragen. Vorgeschrieben ist dazu der AES-128-Standard, der in jedem LoRa-Chip auch hardwareseitig unterstützt ist. Es werden also über ein LoRaWAN-Netzwerk niemals Daten übertragen, die im Klartext lesbar sind. Im folgenden Text interessieren wir uns ausschließlich für Metadaten der LoRaWAN-Kommunikation (NetID, Paketgröße, Spreading Factor, Funk-Kanal, Bandbreite, uä.).

In einigen Situationen wird der Gerätenamen bzw. die ID des Geräts mit übertragen. Dadurch ließe sich in unserem überschaubar großen Verein ein Gerät einer Person zuordnen. Um das zu unterbinden, werden die Geräte-IDs unkenntlich gemacht. Wir haben dies im Arbeitspaket "Anonymisierung" beschrieben.

Die Open Source Software LoRaServer.io (<https://loraserver.io>) enthält ein Modul, mit dem LoRaWAN-Meldungen in MQTT umgewandelt werden (LoRa Gateway Bridge, <https://www.loraserver.io/lora-gateway-bridge/overview/>). Da nun die Meldungen per MQTT verfügbar waren, wurde von uns auf dieser Basis eine Software geschrieben, die MQTT-Meldungen mit LoRaWAN-Paketen einliest, die Geräte-ID anonymisiert, und dann wieder per MQTT weiterreicht. Für unsere Statistiken stehen nun also Daten zur Verfügung, die keine zuordenbaren Geräte-IDs mehr enthält und sonst Metadaten zur Nutzung des Netzes enthält.

Den Code für den “anonymise” findet man in unserem Repository auf Github: <https://github.com/OpenlotNetwork/lora-gateway-bridge-anonymise>

2.4.2. Veröffentlichung der Daten

Die Anonymisierten Daten werden nun in einer influxdb (<https://www.influxdata.com>; Timeseries Database) gespeichert und können zB. über Grafana (<https://grafana.com>) ausgewertet werden.

Aktuell empfangen und verarbeiten wir etwa 100.000 Pakete täglich. Die Plattform ist noch in Entwicklung. An der Veröffentlichung wird noch gearbeitet.

Geplant sind Details zu:

- Verständnis der Nutzung der 8 Standard-Frequenzen (Kanalnutzung)
- Verständnis der Nutzung der Gateways (Anzahl Meldungen)
- Verständnis der Nutzung der Spreading Factors 7-12
- Verteilung der Pakete auf Netze (NetID)
- Paketgrößen
- Empfangsdaten (SNR: Signal-/Rauschabstand)
- zeitlicher Verteilung der Werte

2.4.3. Status des Arbeitspakets

Die Anonymisierung der Daten bewährt sich bereits seit einigen Monaten und liefert zuverlässig Werte. [100%]

Die Auswertung und Veröffentlichung ist noch im Werden. Erste Erkenntnisse stehen zur Verfügung, aber für eine Veröffentlichung ist der Fortschritt noch nicht ausreichend. [50%]

2.5. AP6: Dokumentation

Dieser Bereich gliedert sich in mehrere Aspekte:

- Software: wir haben mehrere Applikationen bzw. Tools entwickelt und als Open Source veröffentlicht. Das ermöglicht anderen Projekten und Communities darauf aufzubauen. Die Dokumentation liegt jeweils den Projekten bei.

Beispiele:

- LoRa GPS Tracker zur Messung der Netzabdeckung: <https://github.com/OpenlotNetwork/LoRa-gpstrack>

- Anonymisierung von Sensordaten, um Auswertungen gem. DSGVO durchführen zu können:
<https://github.com/OpenlotNetwork/lora-gateway-bridge-anonymise>
- Scripts zur vereinfachten Installation bzw. Deployments von Raspberry Pi basierten Gateways:
<https://github.com/OpenlotNetwork/ic880a-setup-scripts>
- Arbeitsgruppen: wir haben zu Beginn unsere Zusammenarbeit über Slack organisiert. Rasch haben wir bemerkt, dass (a) die Akzeptanz von Slack nur mäßig gegeben war, (b) auch öffentliche Mitteilungen nicht zB. über Google gefunden werden und (c) die Meldungen nicht dauerhaft verfügbar sind. Da sich viele Themen wiederholen (zB. Fragen, welche Sensoren wir für gewisse Anwendungen empfehlen können bzw. womit es bereits Erfahrungen gibt), haben wir Ende 2018 ein eigenes Forum etabliert und mittlerweile den Slack-Organisationszugang geschlossen bzw. dorthin migriert:
<https://forum.openiot.network>
- Tätigkeitsbericht: wir möchten unseren Tätigkeitsbericht, den wir für unsere Förderer wie Netidee anfertigen, veröffentlichen, da er sehr gut die Handlungsfelder des Vereins und die Richtungen, die wir verfolgen, widerspiegelt.

Wir verfolgen das Ziel, Erreichtes zu dokumentieren und für zB. Software sämtliche Dokumentation frei zu publizieren.

Ausnahmen sind interne Unterlagen zur Administration des Vereins (Budget/Finanzdaten, Mitgliederlisten inkl. persönlicher Daten und ähnliches). Wir haben das Ziele alle übrige Schriftstücke öffentlich zugänglich zu machen.

2.5.1. Status des Arbeitspakets

Die Plattformen für die Veröffentlichung wurden geschaffen (Website, Forum, Github-Organisationsmitgliedschaft, Mailinglisten) [100%]

Vorhandene Projekte wurden öffentlich dokumentiert. Weitere Projekte sind im Kommen und werden ebenso öffentlich dokumentiert, als auch als Open Source publiziert. [40%]

2.6. AP7: Externkommunikation & Erreichung Sichtbarkeit, Nachhaltigkeit

Externe Kommunikationsmaßnahmen des Projekts verfolgen den Zweck Projektinhalte und Projektfortschritt entsprechend bekannt zu machen, sowie das Wissen über technologische-, fachliche- und kommerzielle Aspekte der LoRaWAN Technologie in Österreich zu fördern. Durch den Aufbau einer breiten Community soll die Hemmschwelle zur Nutzung des aufgebauten Netzwerks für verschiedene Zielgruppen unterstützt und gefördert werden.

Der Fokus wurde dabei im Besonderen auf folgende 3 Zielgruppen gelegt:

Technisch versierte Experten - In dieser Gruppe wurden sowohl Experten als auch angehende Experten adressiert. Zusammenarbeit erfolgt sowohl mit Experten aus dem Bereich LoRaWAN, Experten aus dem Bereich der Funktechnik (z.B.: Österreichischer

Versuchssenderverband), technischen Vereinen (z.B.: Zusammenarbeit mit dem Verein Funkfeuer zur synergetischen Nutzung von strategischen Funkt-Standorten) sowie Universitäten und Fachhochschulen (z.B: Zusammenarbeit mit der Fachhochschule FH Wien sowie der Lauder Business School).

Unternehmen & Institutionen - Unternehmen im Bereich LoRaWAN stellen eine wichtige Zielgruppe der externen Kommunikation dar. Dabei sind sowohl Partnerschaften (z.B.: Firma Nessus) sowie der technologische Austausch.

Beispiele wären:

- Regelmäßiger Austausch Firma Retronic zum Thema Qualität & Verfügbarkeiten von Sensoren und LoRaWAN Geräten.
- Gemeinsamer Workshop mit der Firma Sensor Network Services GmbH auf der Lauder Business School.

Die externen Kommunikationsmaßnahmen wurden in Channels aufgeteilt, die in der Folge beschrieben werden.

2.6.1. Social Media Aktivitäten

Im Bereich Social Media fokussiert das Projekt-Team auf folgende Plattformen:

Twitter

Die Kommunikation des Projekts erfolgt hauptsächlich über die beiden Accounts:

@OpenIoT_network mit 121 Followern

@TTN_Vienna mit 304 Followern

Als Projekterfolg wird gewertet, dass der Ausbau und die Aktivität in den sozialen Medien von Benachbarten Communities erkannt und positiv kommentiert wird:



Als weitere Success-Story hinsichtlich externer Kommunikation gilt der Tweet zur Bekanntmachung der Netidee Förderung, der von @globaldatamaker (108k Followern) geteilt wurde.



Weiters konnte mit der Berichterstattung über den Netidee-Gateway Workshop mit Retweets der Accounts @thethingsntwrk (13,5k Followern) und @IoTbyIMST (1,4k Followern) eine sehr hohe kommunikation Wirkung erzeugt werden.

Verein OpenIoT
@OpenIoT_network

Done! That was easy! Second LoRaWAN #gateway (@IoTbyIMST) of today's #workshop went online!
@netidee @TTN_Vienna @LoRaAlliance @thethingsntwrk

[Tweet übersetzen](#)

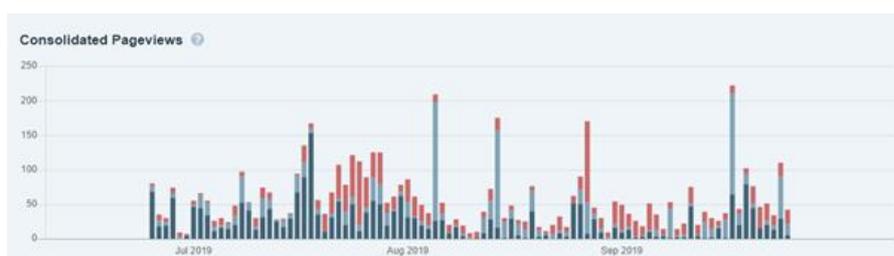


1:52 nachm. · 23. Feb. 2019 aus [Wien, Österreich](#) · [Twitter for iPhone](#)

9 Retweets 18 „Gefällt mir“-Angaben

[Forum \(forum.openiot.at\)](http://forum.openiot.at)

Im Zuge des Projekts wurde ein öffentliches Forum zum nachhaltigen Austausch zu Projektthemen und zur Technologie aufgebaut. Im Schnitt beträgt die monatliche Nutzung bei 1600 Page-Views von über 70 Usern.



2.6.2. Nachhaltigkeit

Ein Projekt-Grundsatz wurde festgelegt, die eigene Software auch als Open Source zu veröffentlichen.

Beispiele dazu: Sensor für Netzreichweitentest (Arduino, 100% Open Source), Akustik-Sensor, Anonymiser-Script für die Anonymisierung von LoRaWAN Geräte IDs.

2.6.3. Status des Arbeitspakets

Konkrete Dokumentation kann zum Ende des Projekts zusammengestellt werden, ebenso Bewertungen und Empfehlungen [30%]

2.7. AP8: Entwicklung von drei Use-Cases

Im Zuge der Netidee-Förderung wurden wir gebeten, drei Use-Cases im Zusammenhang mit unserem Projekt zu erstellen. Wir beschreiben hier drei Use-Cases von uns:

1. Netztestgerät für die Messung der Netzabdeckung
2. Gerätezähler für die Erkennung der Anzahl an WLAN und Bluetooth Geräten in der Nähe (Paxcounter)
3. Akustik-Sensor für die Außenmontage
- 4.

2.7.1. Use Case 1: Netztestgerät

Die Idee war, auf Basis eines Arduino Uno-Geräts mit einem Aufsteckmodul einen GPS-Tracker zu entwickeln, mit dem wir Informationen zur Netzabdeckung generieren.

Seit einigen Jahren gibt es im Internet eine Webseite, die Informationen zur Abdeckung von LoRaWAN-Netzes im Rahmen von The Things Network grafisch abbildet:

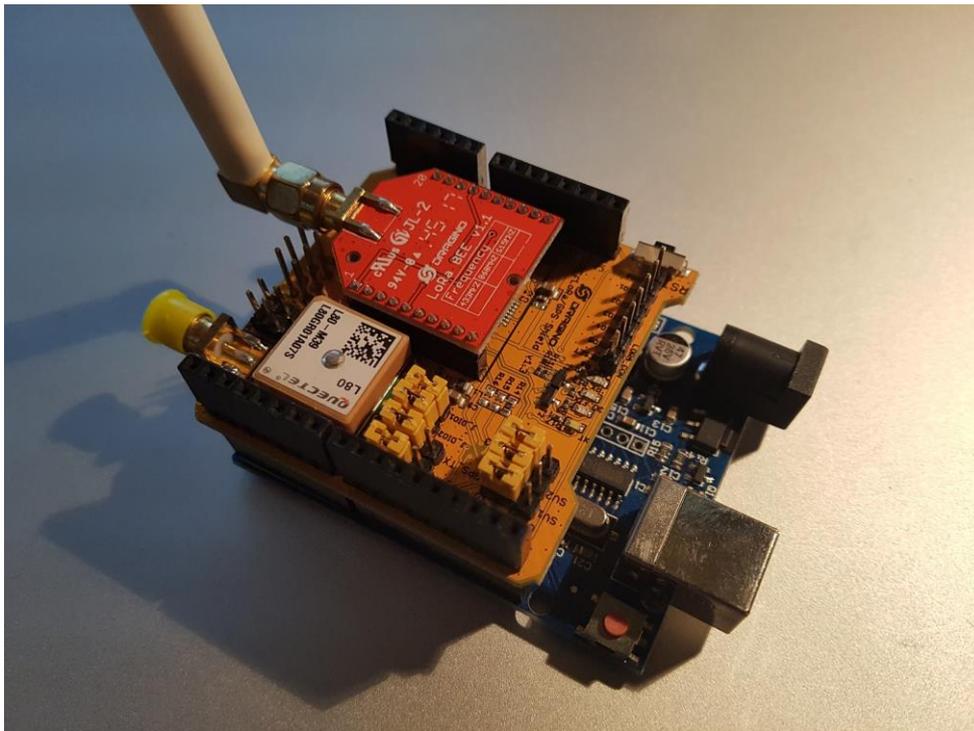
<https://ttnmapper.org/>. Dort wird auch eine Heatmap errechnet, die eine bessere Darstellung ermöglicht. Das Netztestgerät soll zum TTNmapper kompatibel sein, um dort die fertigen Tools nutzen zu können.



Wie erwähnt haben wir auf Basis

- Arduino Uno (<https://store.arduino.cc/arduino-uno-rev3>) und
- Dragino LoRa GPS Shield (<https://www.tindie.com/products/edwin/loragps-shield-for-arduino/>)

Software entwickelt, die zyklisch Positionsdaten sendet, sobald ein GPS Signal verfügbar ist. In dem LoRaWAN-Paket sind auch Informationen zu den Gateways enthalten, die das Paket empfangen haben. Daraus kann die Reichweite festgestellt werden. Die Daten helfen auch bei der Netzwerkplanung, weil darüber die Reichweite der einzelnen Gateways bekannt ist, inkl. der Auswirkungen, falls es zu einem Ausfall kommt.

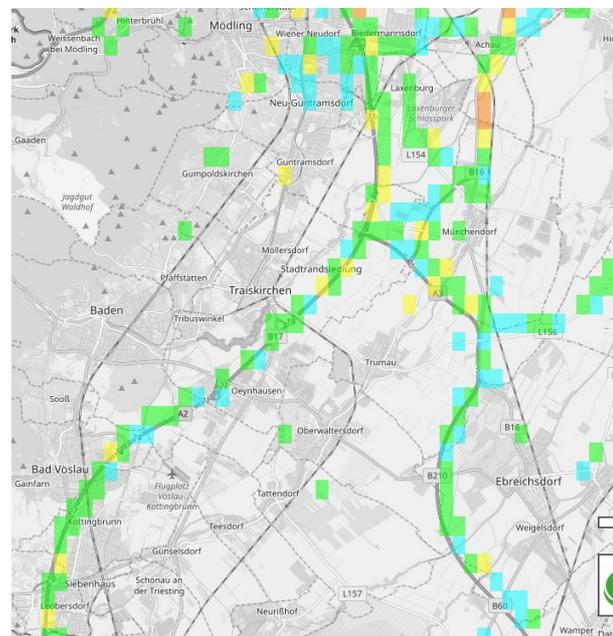


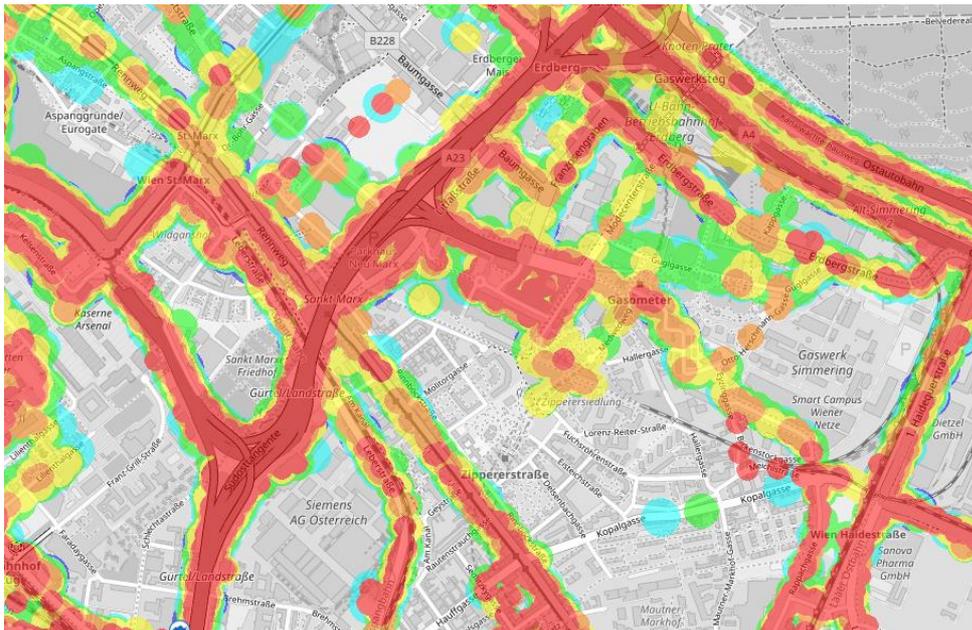
Die Software haben wir als Open Source auf Github veröffentlicht:
<https://github.com/OpenlotNetwork/LoRa-gpstrack>

Der Software liegt auch eine kleine Dokumentation für den Nachbau des Sensors und die Konfiguration der Einstellungen bei.

Das Netzwerktestgerät haben wir mehrfach gebaut und teilweise in unsere KFZ integriert. Bei jeder Fahrt wird mit der Zündung das Testgerät aktiviert und während der Fahrt die Reichweite gemessen. Das passiert ohne Aufwand für den Fahrer/die Fahrerin.

Hinweis zur Auswertung: wir haben erkannt, dass Straßen wesentlich häufiger gemessen werden, als die übrigen Bereiche. Das ist bei der Interpretation der Karten wichtig: die Karten zeigen nur Bereiche in denen gemessen wurden. Das bedeutet, dass die freien Flächen dazwischen möglicherweise ähnlich gut funktionieren, die die umgebenden Messergebnisse zeigen. Es wurde an den freien Flächen einfach noch nicht gemessen.



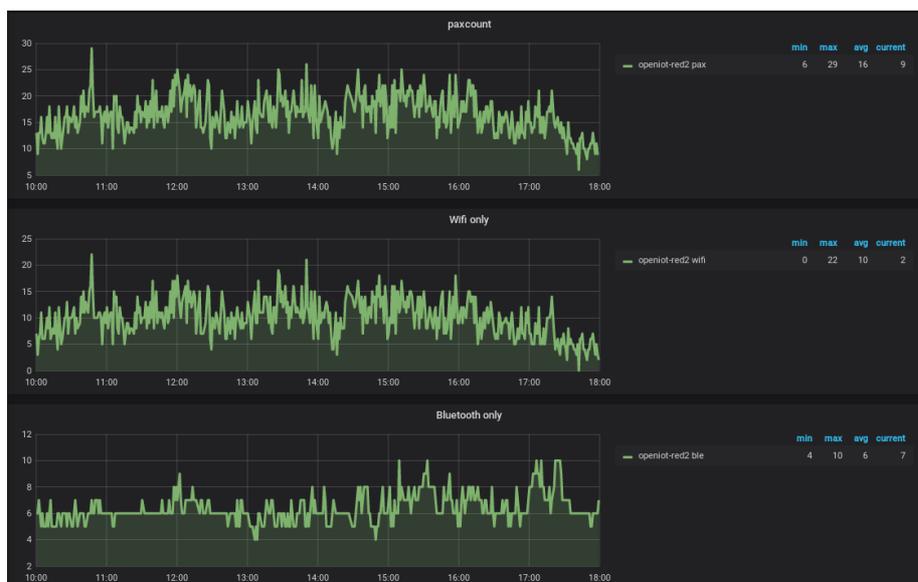


2.7.2. Use Case 2: Gerätezähler (Paxcounter)

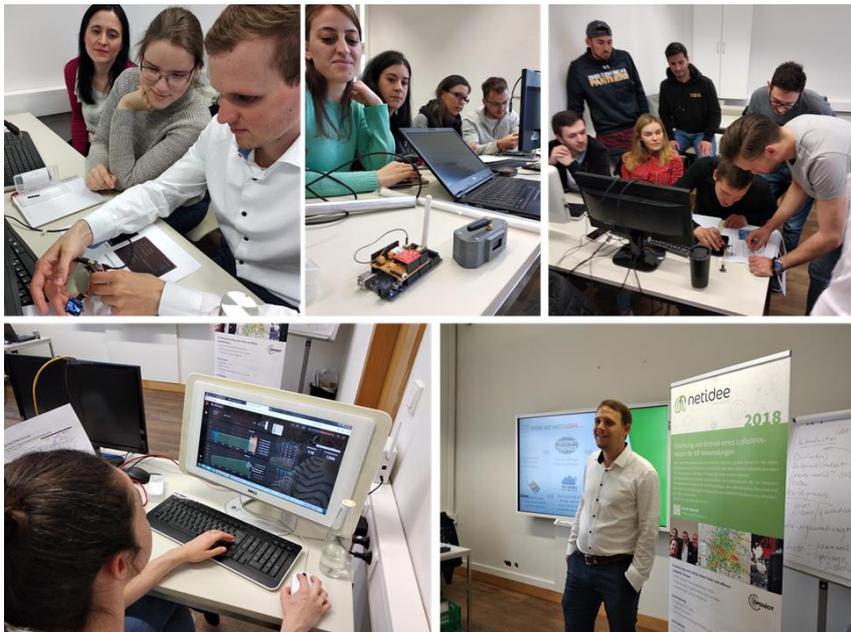
Als eine Anwendung für LoRaWAN wurde die Evaluierung des Paxcounter in den Projektscope aufgenommen. Diese Anwendung zählt die Personen, bei denen WLAN und BLE (Bluetooth Low Energy) aktiviert ist. Die Werte lassen sich separat auswerten und über LoRaWAN übertragen.

Die Anwendung wurde im Zuge des Projekts an 3 Stellen evaluiert:

- Verifikation der Anzahl der Besucher und Interessenten eines Standes während der Raritätenbörse im Botanischen Garten in Wien am 14.04.2019.



- LoRaWAN Workshop der Lauder Business School gemeinsam mit der Firma Sens Networks am 06.05.2019



- Messung einer Freiluft Kino Vorstellung im Zuge des Bunten Sommers Korneuburg am 12.08.2019 mit 3 Messpunkten.



2.7.3. Use Case 3: Akustik-Sensor

Ziel ist ein batteriebetriebener Außensensor zur Geräuschpegelmessung. Der Bauplan und der Code wird auf Github veröffentlicht.

Im Zuge des Aufbaus wird ein Workshop veranstaltet, bei dem etwa 15 Sensoren gebaut werden sollen.

Die Auswertung soll den Geräuschpegel für die jeweiligen Standorte auf einer Karte anzeigen.

2.7.4. Status des Arbeitspakets

Das Netztestgestät aus Use Case 1 ist abgeschlossen und bewährt sich seit Monaten in einigen KFZ und auf Fahrrädern oder tragbaren Sensoren. [100%]

Die Integration des Paxcounter (InfluxDB, Grafana) funktioniert, auch zwei Events wurden bereits damit betrachtet. Die Auswertung ist noch nicht vollständig. [70%]

Das Konzept und die Bill of Material sind festgelegt. Die Hardware ist größtenteils schon geliefert. Der Sensor soll vor dem Winter bereit sein, um bereits Erfahrungen durch den Winter sammeln zu können - diese können beim Outdoor-Sensor hilfreich für mögliche Verbesserungen 2020 sein. [30%]

2.8. AP10: Errichtung einer IoT Plattform

Über das LoRaWAN-Netzwerk werden Daten generiert, die ausgewertet werden wollen. Auch für die Abbildung von Use-Cases benötigt es eine Plattform, um die Daten miteinander zu verknüpfen und darzustellen. Je nach Anwendungsfall sollen auch Aktionen, Alarmer, Emails oder andere Ereignisse ausgelöst werden.

Neben den Use-Cases benötigt die Verwaltung des Netzes, das Monitoring und Reporting-Funktionen Ressourcen.

Für die Verwaltung des Vereins haben wir eine kleine Umgebung geschaffen, in der wir gemeinsam arbeiten können. Beispiele sind Systeme für den Datenaustausch bzw. Dateiablagen für die gemeinsamen Projekte. Auch ein Forum für den Austausch zwischen den Projektmitarbeitern, Mitgliedern und Interessierten wird dort betrieben.

Ziel der Plattform ist somit:

- eine gemeinsame, tragfähige Infrastruktur für unsere Anforderungen
- Betrieb, Monitoring und Reporting des LoRaWAN-Netzes und der Infrastruktur
- Auswertung der Messdaten und Abbildung der Use Cases
- Ecosystem für die Administration, Zusammenarbeit

2.8.1. Infrastruktur

Um im IoT-Bereich eine Plattform zu schaffen, die Flexibilität und Unabhängigkeit bietet, haben wir uns viel Gedanken zur Architektur gemacht. Dankenswerterweise hat uns Fa. Nessus Unterstützung zukommen lassen, wodurch wir unsere Server und Netzwerkgeräte (va. Router und Switches) in einem professionellen Rechenzentrum housing können. Durch das physische Housing haben wir die Möglichkeit, unsere Services sowohl von der Netzwerkseite als auch Applikationsseitig von der Virtualisierung an selbst zu definieren. Über die Anmeldung als LIR bei RIPE NCC haben wir auch Ressourcen (IP-Adressen, ASN) für die Nutzung und Anbindung an das Internet erhalten. Vor allem da nicht auszuschließen ist, dass einzelne Adressen "hard coded", also dezentral fix konfiguriert sein müssen, ist es wichtig, hier als LoRaWAN-Netzbetreiber unabhängig zu sein. Auch, um die Anbindung über mehrere ISPs zu ermöglichen.

Aktuell betreiben wir drei Server, zwei Switches und zwei Router im Rechenzentrum bei Nessus. Alle von uns angebotenen Services laufen darüber. Unsere Webseite ebenso wie das Forum oder die Plattform zur Verarbeitung der LoRaWAN Pakete und Daten von Sensoren.

2.8.2. Systeme für Betrieb, Monitoring und Reporting des LoRaWAN Netzes

Wie in anderen Kapiteln dieses Berichts erwähnt, nutzen wir Ansible und Zabbix für Configuration Management und Monitoring/Reporting unserer Gateways. Die Systeme dafür werden auf der Plattform gehostet und betrieben.

2.8.3. Auswertung der Messdaten

Für die Auswertung der Messdaten stehen mehrere Systeme und "Stacks" zur Verfügung:

- redundanter RabbitMQ Message Broker
- ELK-Stack: Elasticsearch, Logstash, Kibana
- Grafana für Reporting
- NodeRed zum Empfangen, Bearbeiten und Verschneiden der Dateninhalte
- Datenbankserver wie MongoDB oder MariaDB
- LoRaServer.io Gateway Bridge für das anonyme Monitoring von Echtzeiten aus dem LoRaWAN-Netzwerk

Diese Systeme werden in mehreren Projekten als gemeinsame Infrastruktur genutzt.

2.8.4. Ecosystem für Administration und Kollaboration

Einige Dienste für den Verein und unser Vorhaben werden ebenfalls auf dieser Plattform betrieben, beispielsweise:

- Webseite (<https://openiot.network>)
- Forum (<https://forum.openiot.network>)
- Nextcloud für Datenaustausch
- Netzwerkmanagement (NMS) für Monitoring per SNMP und Alarmierungen
- Identity Management Plattform (IDM) für Benutzerverwaltung und Single-Sign-On
- redundanter Firewall Cluster für die Trennung der Netzzonen
- Windows-Terminal-Server für unsere Anwendungen
- Backup-System für automatische Datensicherung lokal und Überspielung zu entfernten Standorten für Disaster Recovery

2.8.5. Status des Arbeitspakets

Drei Ziele wurden für die IoT Plattform definiert:

Ergebnis 1: Kommunikation mit Gateways wurde umgesetzt ist seit mehreren Monaten aktiv. Neben der Übermittlung der Daten ist auch das Management der Gateways umgesetzt. [100%]

Ergebnis 2: Sichere Verarbeitung der Daten: die Plattform ist mittlerweile in der Lage die Daten sicher und zuverlässig zu verarbeiten. Statistiken werden seit Monaten kontinuierlich generiert. [100%]

Ergebnis 3: Visualisierung der Daten: hier gibt es im Hintergrund große Fortschritte, wir veröffentlichen viele der vorhandenen Daten allerdings noch nicht. Für diesen Schritt

möchten wir noch etwas Erfahrung in der Auswertung sammeln, die Ergebnisse besser aufbereiten und IT Security nochmal bewusst betrachten. [40%]