Sicherheitsstudie Ladeinfrastrukturanbindung

Steuerung von Ladeinfrastruktur durch CPOs und Aggregatoren

Autor_innen:

Dr. Joachim Fabini, DI Alexander Hartl, DI Fares Meghdouri, Prof Dr Tanja Zseby

TU Wien, Institute of Telecommunications
Gußhausstraße 25/E389, 1040 Wien

Kurzfassung

Mit der steigenden Anzahl von E-Fahrzeugen geht der Bedarf einer flächendeckend ausgebauten, leistungsfähigen und verlässlichen Ladeinfrastruktur einher, sowohl in Privathaushalten als auch im (halb-)öffentlichen Raum. Dem Ausbau der Ladeinfrastruktur sind vor allem durch die hohen Leistungen der Ladestationen sowie durch beträchtliche Investitionen in den Ausbau und der Erweiterung der verfügbaren Niederspannungs- und Mittelspannungsnetzinfrastruktur Grenzen gesetzt. Neben einem Ausbau der Netzkapazität sind deshalb kurzfristig umsetzbare Maßnahmen zu evaluieren, um mit technischen Mitteln die Netzstabilität aufrecht zu erhalten und die Auswirkung von möglichen Leistungsengpässen auf die Wahrnehmung von Kund_innen zu minimieren.

Diese Studie analysiert die Sicherheit und mögliche Angriffsflächen, sowie die Gefährdungen der Privatsphäre im Falle der Fernsteuerung von Ladestationen („Smart Charging“) für E-Fahrzeuge bei Kund_innen durch Ladestationsbetreiber (Charge Point Operator, CPO). Viele Energielieferanten haben seit mehr als zehn Jahren bereits als CPO umfangreiche Erfahrungen im Betrieb von Ladestationen bzw. dem Lastmanagement im (halb-)öffentlichen Raum gesammelt. Ladestationen von Privatkund_innen werden bisher nicht durch CPOs gesteuert, bieten jedoch angesichts der hohen Steigerungsraten und zunehmenden Ladeleistungen ein großes Potential zur Netzstabilisierung. Herausforderung bei der Steuerung von Ladestationen von Privatkund_innen sind unter anderem die sichere Kommunikation zwischen CPO und Ladestation, die Koexistenz der Ladestationssteuerung mit diversen SmartHome-Geräten im Kommunikationsnetz (LAN) der Kund_innen und Themen betreffend Datenschutz-Grundverordnung (DSGO) und Privatsphäre. Sicherheit im Kontext der Kommunikationsnetze beinhaltet die sogenannte CIA-Triade, bestehend aus Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability). Eine Verschlüsselung mit dem Ziel der Vertraulichkeit ist notwendig, um passives Abhören der Kommunikation zwischen Ladestation und CPO durch Angreifer zu unterbinden. Die Integritätssicherung der Kommunikation zwischen Ladestation und CPO beugt Angriffen durch sogenannte Man-in-the-Middle (MitM) vor, die andernfalls Datenwerte verfälschen oder falsche Steuersignale generieren könnten. Die Verfügbarkeit ist eine wesentliche Voraussetzung dafür, dass ein CPO im Anlassfall (z.B. bei Leistungsengpässen) tatsächlich die Ladestationen von Kund_innen erreichen und schnell und effizient regelnd eingreifen kann.

Auf technischer Ebene hat sich mit dem von der OpenChargingAlliance (OCA) standardisierten Open Charging Point Protocol (OCPP) in den Versionen 1.6 bzw. 2.0.1 zum Zeitpunkt des Verfassens der Studie (Q1 2023) ein offener Standard für die Kommunikation des CPOs mit Ladestationen etabliert. Auch wenn Aktivitäten zur Standardisierung potentieller Nachfolgeprotokolle wie beispielsweise IEC 63110 gestartet wurden, bevorzugen Entscheidungsträger aus Politik und Wirtschaft den Einsatz des offenen OCPP-Standards zum Ausbau der Ladeinfrastruktur.

Schwerpunkt der Studie ist demzufolge die Analyse der Sicherheit und Privatsphäre der Fernsteuerung von Ladestationen bei Kund_innen durch CPOs unter Verwendung des Protokolls OCPP. Weitergehend werden zu erwartende Antwortzeiten dieser Ansteuerung evaluiert um die technische Machbarkeit und Funktionalität dieser Steuerungsform zu beurteilen.

Die ausführliche Recherche vorhandener wissenschaftlicher Publikationen und Standards zum Themenblock „Sicherheit von Ladeinfrastrukturen“ kommt zum Schluss, dass zum Zeitpunkt des Verfassens der Studie keine wesentlichen Schwachstellen von OCPP bekannt sind, die einem sicheren Steuern von Ladestationen widersprechen. Die Standardisierung von OCPP hat in den letzten Versionen (OCPP-J 1.6 mit Sicherheitserweiterungen sowie 2.0.1) wichtige Nachbesserungen im Bereich Sicherheit vorgenommen. Die OCPP-Sicherheitsprofile 2 (TLS mit Server-Zertifikat) sowie 3 (TLS mit Server- und Client-Zertifikat) sehen eine verpflichtende Ende-zu-Ende Verschlüsselung mittels Transport Layer Security (TLS) vor. TLS in der Version 1.2 und Nachfolgeversion 1.3 gewährleisten bei

der Verwendung geeigneter kryptographischer Verfahren (Ciphers) eine grundsätzliche, notwendige Voraussetzung für die sichere Ladestationssteuerung.

Eine Analyse möglicher Varianten der Ladestationssteuerung hat high-level Bedrohungsszenarien ergeben, die durch geeignete Gegenmaßnahmen verhindert werden müssen:

1. Ein Angreifer kann die notwendige Steuerung von privaten Ladestationen durch den CPO erschweren, stören oder unterbinden
2. Ein Angreifer kann aufgrund von Sicherheitslücken Ladestationen übernehmen und regeln.
3. Ein Angreifer erreicht die Punkte (1) und (2) für eine große Anzahl von Ladestationen.
4. Ein Fernzugriff auf die Ladestation durch Angreifer oder CPO gefährdet die Privatsphäre der Kund_innen.

Auf technischer Ebene ist die Architektur der Vernetzung zwischen dem Backend (Charge Point Management System, CPMS) des CPO und der Ladestation von Kund_innen ein wesentlicher Faktor für die Einschränkung möglicher Angriffs- und Abwehrmöglichkeiten. Die Studie untersucht demzufolge vier mögliche Anwendungsfälle, im Detail: **AF0**: Offline-Ladestation, **AF1**: Ladestation mit Mobilfunk-Anbindung, **AF2**: Ladestation mit Anbindung über das Kund_innen LAN bzw. dessen vorhandene Internet-Anbindung, sowie **AF3**: Ladestation mit gleichzeitiger Anbindung über Mobilfunk und das Kund_innen LAN bzw. -Internet.

Auf Protokollebene kommt die Studie zum Schluss, dass sich OCPP 2.0.1, bzw OCPP-J 1.6 (JSON/Websocket) mit Sicherheitserweiterungen bei Verwendung des OCPP-Sicherheitsprofils 3 für eine sichere Ladestationssteuerung durch den CPO eignen. Sofern Zusatzbedingungen erfüllt sind – jede Ladestation muss einen eindeutigen, geheimen, den Angreifern nicht bekannten und von ihnen nicht erratbaren Schlüssel speichern – ist auch das OCPP-Sicherheitsprofil 2 für eine sichere Ladestationssteuerung geeignet, vergrößert jedoch die mögliche Angriffsfläche des CPOs bzgl. Verfügbarkeit. Während bei Verwendung des OCPP-Sicherheitsprofils 3 ein CPO die Verbindungsversuche von Angreifern bereits beim TLS-Verbindungsaufbau abblocken kann, gelingt ihm das bei OCPP-Sicherheitsprofil 2 nur zu einem späteren Zeitpunkt, bei der verpflichtenden Authentifizierung der Ladestation. Dieses Kriterium kann bei der erfolgreichen Abwehr von Distributed Denial-of-Service Angriffen mit Malware und Botnetzen entscheidend sein. Von der Verwendung von OCPP-S 1.6 oder früheren Versionen (basierend auf SOAP/XML) wird explizit abgeraten, da u.a. der Standard OCPP keine (ausreichenden) standardisierten Sicherungsmaßnahmen definiert.

Auf architektureller Ebene ist das Ergebnis der Studie, dass AF1 (Ladestation mit Mobilfunk-Anbindung unter Verwendung eines privaten Access Point Name (APN) und mit zusätzlichen Sicherungsmaßnahmen) aus Sicht der Vertraulichkeit, Integrität und Verfügbarkeit, bzw. vor allem bezüglich Wahrung der Privatsphäre von Kund_innen die meisten Vorteile bietet. Wesentliche Nachteile sind Kosten für den CPO sowie Schwierigkeiten bei fehlender Funkversorgung (Tiefgaragen, ländlicher Bereich mit schwachem Mobilfunkempfang). Als Alternative bietet sich AF2 (Anbindung über Internet-Modem und LAN von Kund_innen) in der Variante 1 an (Kund_innen können nicht lokal auf ihre Ladestation zugreifen, Ladestations-Zugriff läuft ausschließlich über CPO). Die Wahrung der Privatsphäre der Kund_innen erfordert jedoch technische Lösungen, um die Ladestation in einem eigenen virtuellen LAN (VLAN) oder WLAN vom LAN der Kund_in zu isolieren. Andernfalls haben Kund_innen keine technische Möglichkeit zu verhindern, dass der CPO den Zugriff auf die Ladestation missbraucht, um das (W)LAN von Kund_innen und deren Verhalten auszukundschaften. Die letzte Aussage gilt gleichermaßen für AF 2 Variante 2 (Kund_innen können auf Ladestation lokal, direkt zugreifen) sowie für AF3. Desgleichen gefährden AF2 und AF3 (ohne VLAN-Abschottung der Ladestation) die Sicherheit der Ladestation: kompromittierte Geräte im Kund_innen-LAN können die Ladestation auskundschaften, versuchen deren Schwachstellen zu identifizieren und angreifen. AF0

(Offline-Ladestation) wird aufgrund regulatorischer Erfordernisse (Technische und Organisatorische Regeln für Betreiber und Benutzer von Netzen, TOR Verteilernetze) ab 2025 nicht mehr zulässig sein.

Die Evaluierung der Messungen in realen Mobilfunknetzen erlaubt eine Abschätzung möglicher Antwortzeiten der Ladestation bei einem Steuerbefehl des CPO an die Ladestation. Diese Antwortzeiten sind abhängig von der Größe des Steuerbefehls, der verwendeten Mobilfunktechnologie, sowie von der Zeit der Inaktivität der Mobilfunkverbindung vor dem Absetzen des Steuerbefehls durch den CPO. Festgestellt wurde, dass kurze Zeiten der Inaktivität (ca. 30 Sekunden keine Datenübertragung) bei Mobilfunknetzen zu einer deutlichen Erhöhung der Übertragungszeit beim ersten Steuerpaket führen. Für einen als realistisch erachteten Fall wurde für einen 1500 Byte großen Steuerbefehl, je nach Funktechnologie, eine mittlere Rundlaufzeit (Round-trip delay) von ca. 0,65 Sekunden für 4G, 1,8 Sekunden für 3G sowie 3 Sekunden für 2G Netze ermittelt. Bei Verwendung von drahtgebundenen Netzen (VDSL, Kabel) ist von deutlich geringeren Laufzeiten auszugehen, d.h. die 3 Sekunden (zuzüglich Bearbeitungszeit der Ladestation) für 2G geben eine obere Schranke für zu erwartende Antwortzeiten an.

Zusammenfassend stellt die Studie fest, dass OCPP bei Berücksichtigung der empfohlenen Sicherheitsmaßnahmen eine sichere Möglichkeit der Leistungssteuerung von Ladestationen bei Privatkund_innen durch den CPO bietet, mit vielversprechendem Potential für die Netzstabilisierung.

Abstract

The huge success and a steadily increasing number of e-vehicles in Austria results in the need for a comprehensive, high-performance and reliable charging infrastructure, both in private households and in (semi-)public spaces. The required extension of the charging infrastructure is challenged, among others, by the high charging capacity of charging stations and by the need for enhancements to the existing low-voltage and medium-voltage grid infrastructures. In addition to a long-term increase of the overall grid capacity, alternative short-term measures must be evaluated that support grid stability by technical means and minimize the impact of possible power bottlenecks onto customer perception. However, the electricity grid is a critical infrastructure and therefore a tempting target for attackers. The protection of the grid's IT components against cyberattacks is essential to ensure the secure transmission of sensor data and control actions

This study analyzes the security and potential attack surfaces, as well as privacy threats in the case of "smart charging", in particular considering the remote control of e-vehicle charging stations of residential customers by charging point operators (CPOs). Many energy suppliers have already gained extensive experience as CPOs in the operation of charging stations and load management in (semi)public spaces for more than ten years. Charging stations of residential customers have not been controlled by CPOs so far, but offer great potential for grid stabilization in view of the high growth rates and increasing charging capacities. Challenges in controlling residential charging stations include secure communication between CPOs and charging stations, coexistence of charging station control with various smart home devices in the customer's local communication network (local area network, LAN), as well as conformance to the General Data Protection Regulation (GDPR) and privacy demands. Security in the context of communication networks includes the so-called CIA triad, consisting of the security objectives confidentiality, integrity and availability. Encryption with the goal of confidentiality is necessary to prevent passive eavesdropping of the communication between charging station and CPO by attackers. Integrity assurance of the communication between charging station and CPO prevents attacks by so-called man-in-the-middle (MitM), who could otherwise falsify data values or generate false control signals. Availability is essential for the CPO to always have timely access to charging station status and to actually control them. These are two main prerequisites that enable the CPO to intervene quickly and efficiently for stabilizing the grid in the case of an incident (e.g., power bottleneck).

At a technical level, the Open Charging Point Protocol (OCPP) standardized by the OpenChargingAlliance (OCA) in versions 1.6 and 2.0.1 respectively has established an open standard for the communication of the CPO with charging stations at the time of writing (Q1 2023). Even though activities have been started to standardize potential successor protocols such as IEC 63110, decision makers from politics and industry prefer to use the open OCPP standard to expand the charging infrastructure.

Accordingly, the focus of this study is to analyze the security and privacy of remote control of charging stations at customers by CPOs using the OCPP protocol. Furthermore, the expected response times of this control mechanism are evaluated in order to assess its technical feasibility and functionality.

The extensive research of existing scientific publications and standards on the topic of "security of charging infrastructures" concludes that, at the time of writing, no significant weaknesses of OCPP are known that could question a secure control of charging stations. The standardization of OCPP has made important improvements in the area of security in the last versions (OCPP-J 1.6 with security enhancements as well as 2.0.1). OCPP security profiles 2 (TLS with server certificate) and 3 (TLS with server and client certificate) demand for mandatory end-to-end encryption using Transport Layer

Security (TLS). TLS version 1.2 and its successor version 1.3 ensure a basic, necessary prerequisite for secure charging station control when suitable cryptographic methods and ciphers are used.

The analysis of possible variants of charging station control has revealed high-level threat scenarios that must be prevented by suitable countermeasures:

1. An attacker can impede, disrupt or prevent the necessary control of private charging stations by the CPO.
2. An attacker can compromise and control charging stations due to security vulnerabilities.
3. An attacker achieves points (1) and (2) for a large number of charging stations.
4. Remote access to the charging station by an attacker or CPO compromises customer privacy.

At a technical level, the architecture of the communication path that connects the CPO's backend (Charge Point Management System, CPMS) and the customer's charging station is a key factor in restricting possible attack options The study therefore examines four possible use cases, in detail: AF0: offline charging station, AF1: charging station with mobile radio connection, AF2: charging station with connection via the customer's LAN or its existing Internet connection, and AF3: charging station with simultaneous connection via mobile radio and the customer's LAN or Internet.

At the protocol level, the study concludes that OCPP 2.0.1, or OCPP-J 1.6 (JSON/Websocket) with security extensions when using OCPP security profile 3, are suitable for secure charging station control by the CPO. If additional conditions are met - each charging station must store a unique, secret key that is not known to and cannot be guessed by attackers - OCPP security profile 2 is also suitable for secure charging station control, but increases the CPO's potential attack surface in terms of availability. While a CPO using OCPP security profile 3 can already block the connection attempts of attackers during the TLS connection setup, with OCPP security profile 2 it can only do so at a later point in time, during the mandatory authentication of the charging station. This criterion can be crucial in successfully defending against distributed denial-of-service attacks by malware and botnets. The use of OCPP-S 1.6 or earlier versions (based on SOAP/XML) is explicitly discouraged because, among other deficiencies, the OCPP standard does not define (sufficient) standardized security measures.

At an architectural level, the study identified that AF1 (charging station with mobile connection using a private access point name (APN) and with additional security measures) offers most benefits from the point of view of confidentiality, integrity and availability, and especially with regard to protecting the privacy of customers. The main drawbacks are costs for the CPO and difficulties in the absence of radio coverage (underground garages, rural areas with weak mobile reception). An alternative is AF2 (connection via Internet modem and customer LAN) in variant 1 (a subcase of AF2: customers cannot access their charging stations locally, but only via CPO). However, protecting the privacy of customers requires technical solutions to isolate the charging station in its own virtual LAN (VLAN) or WiFi from the customer's LAN. Otherwise, customers have no technical way to prevent the CPO from abusing access to the charging station to spy on customers' LAN/WiFi and their behavior. The last statement applies equally to AF 2 variant 2 (customers have local access to their charging stations) and to AF3. Similarly, AF2 and AF3 (without VLAN isolation of the charging station) endanger the security of the charging station: compromised devices connected to the customer's LAN can explore the charging station, try to identify its vulnerabilities and attack it. AF0 (offline charging station) will no longer be allowed from 2025 due to regulatory requirements (Austrian Technical and Organizational Rules for Operators and Users of Networks, TOR Verteilernetze).

The evaluation of measurements in real mobile networks allows an estimation of possible response times of the charging station in case of a control command sent by the CPO to the charging station. These response times depend on the size of the control message, the cellular technology used, and the time of inactivity of the cellular connection before the CPO sends the control command. One finding

was that short periods of inactivity (about 30 seconds of no data transmission) for cellular networks lead to a significant increase in transmission time for the first control packet. For a case considered realistic, an average round-trip delay of about 0.65 seconds for 4G, 1.8 seconds for 3G, and 3 seconds for 2G networks was determined for a 1500-byte control command, depending on the radio technology. When using wireline networks (VDSL, cable), significantly lower round-trip times can be assumed, i.e., the 3 seconds (plus charging station processing time) for 2G indicate an upper bound for expected response times.

In summary, the study finds that, if the recommended security measures are considered, OCPP offers a secure way for the CPO to control charging stations at residential customers, with promising potential for network stabilization.

Inhaltsverzeichnis

1 Ladeinfrastruktur: Einleitung und Überblick

1.1. Hintergrund und Inhalt der Studie

Gestiegenes Umweltbewusstsein, technologischer Fortschritt, Veränderungen der Kostenstruktur sowie umfassende Förderprogramme auf nationaler und EU-Ebene sind nur einige der Erfolgsfaktoren, die in den letzten Jahren zu signifikanten Steigerungsraten in der Elektromobilität geführt haben [1], [2]. Fahrzeuge mit elektrischem Antrieb können bei Versorgung auf der Basis von Strom aus erneuerbaren Energien die Abhängigkeit des Verkehrssektors von fossilen Brennstoffen deutlich verringern, CO2-Emissionen vermeiden und die Energieeffizienz deutlich steigern.

Mit der steigenden Anzahl von E-Fahrzeugen einher geht der Bedarf einer flächendeckend ausgebauten, leistungsfähigen und verlässlichen Ladeinfrastruktur sowohl in Privathaushalten als auch im (halb-)öffentlichen Raum. Dem Ausbau der Ladeinfrastruktur sind vor allem durch die hohen Leistungen der Ladestationen sowie durch beträchtliche Investitionen in den Ausbau und der Erweiterung der verfügbaren Niederspannungs- und Mittelspannungsnetzinfrastruktur Grenzen gesetzt. Gängige Ladeleistungen reichen von 11 kW und 22 kW bei Wechselstrom-Ladestationen (AC) über 350 kW bei Gleichstrom-Ladestationen (DC) bis zu geplanten 1,5 MW für den Schwerverkehr. Dem gegenüber steht ein mittlerer Leistungsbedarf eines österreichischen Haushalts von rund 4 kW, für dessen Versorgung die bestehende Verteilernetzinfrastruktur dimensioniert wurde und den heutigen und künftigen Anforderungen nicht mehr ausreichend gerecht wird. Zur Erreichung der Klimaziele bedarf es einer signifikanten Elektrifizierung aller Wirtschaftssektoren und demnach auch dem Ausbau und der Verstärkung der Netzinfrastruktur.

Neben einem Ausbau der Netzkapazität sind kurzfristig umsetzbare Maßnahmen notwendig, um mit geeigneten technischen Mitteln den erforderlichen Ausbau der Ladeinfrastruktur zu ermöglichen, im Rahmen der verfügbaren Netzkapazitäten. Ziel dieser Maßnahmen ist es, einerseits die Netzstabilität aufrecht zu erhalten und andererseits die Auswirkung von tatsächlichen Leistungsengpässen auf die Wahrnehmung von Kund_innen zu minimieren.

Eine Option dafür ist die Steuerung von Lasten bei Endverbraucher_innen (Kund_innen) wie z.B. Ladestationen für Elektrofahrzeuge (sogenanntes „Smart Charging“), Wärmepumpen, elektrische Heizungen und Warmwasseraufbereitung. Diese Möglichkeit beruht jedoch auf vier wesentliche Voraussetzungen:

1. Die zu steuernde Last (z.B. Ladestation) muss die technische Anforderung der Fernsteuerung erfüllen.
2. Die notwendige Kommunikations-Infrastruktur muss vorhanden sein, um einem Ladestationsbetreiber (Charge Point Operator, CPO) einen steuernden Zugriff auf die Last zu ermöglichen.
3. Der Einfluss der Steuerungsmaßnahme auf die Bedürfnisse und den Komfort der Kund_innen muss minimiert werden.
4. Sicherheit und Privatsphäre der beteiligten Parteien dürfen durch die Steuerung nicht beeinträchtigt werden. Das betrifft sowohl die Sicherheit und Privatsphäre der Kund_innen gegenüber dem CPO und vice versa sowie – als wesentliche Komponente – von CPO und Kund_innen gegenüber potentiellen Angreifern.

Diese Studie analysiert die Sicherheit und mögliche Angriffsfläche der Kommunikation sowie die Gefährdung der Privatsphäre im Falle der Fernsteuerung von Ladestationen für E-Fahrzeuge bei Kund_innen durch Ladestationsbetreiber (CPO)**.** Viele Energielieferanten haben seit mehr als zehn

Jahren bereits als CPO umfangreiche Erfahrungen im Betrieb und zunehmend auch in der Steuerung von Ladestationen bzw. dem Lastmanagement im (halb-)öffentlichen Raum gesammelt. Anfängliche Sicherheitslücken in Implementierungen der Ladestationen ([3]) wurden mittlerweile geschlossen und mit dem Open Charging Point Protocol (OCPP) [4] in den Versionen 1.6 bzw. 2.0.1 hat sich zum Zeitpunkt des Verfassens der Studie (Q1 2023) ein offener Standard für die Kommunikation mit Ladestationen etabliert.

Anlässlich der technischen Diskussionen bzw. Analyse und Evaluierung der Ansteuerung von Ladestationen hat sich gezeigt, dass für die gesamtheitliche Betrachtung der Problemstellung zahlreiche Themenstellungen von Relevanz sind, die allerdings über die sicherheitstechnische Betrachtung hinaus gehen und außerhalb des Rahmens dieser Studie liegen, insbesondere:

1. **Regulatorische Rahmenbedingungen für die Nutzung von Flexibilitäten im Energie- und Stromsystem:** Die Frage der Ansteuerung von Ladestationen stellt einen Teilaspekt einer deutlich umfassenderen Debatte im Rahmen der Transformation des Energiesystems dar, nämlich jene der Schaffung von Rahmenbedingungen für die Nutzung von Flexibilitäten in der Niederspannung und den entsprechenden Regelungen zur Flexibilitätserbringung basierend auf dem bestehenden Marktmodell, inklusive Fragestellungen betreffend die **bidirektionale Energieübertragung Vehicle-to-Grid (V2G)** bzw. Vehicle-to-X (V2X) – d.h. Einbindung von Batterien der Elektrofahrzeuge als Speicherquelle. Die vorliegende Studie beschränkt sich ausschließlich auf die (unidirektionale) Steuerung zwecks Reduktion der Ladeleistung.
2. **Dimensionierung und Digitalisierung der Stromnetze**: Messungen im Niederspannungsbereich, Sensorik und Logik der Erkennung einer drohenden Gefährdung der Versorgungssicherheit und einer Notwendigkeit der Steuerung bei Kund_innen.
3. **Technische Machbarkeit der Ansteuerung**: werden regulatorische Rahmenbedingungen geschaffen, um das Zeitintervall zwischen zwei Abfragen der Ladestation kürzer als die derzeit bei Smart Meter gültigen mindestens 15 Minuten zu ermöglichen? Voraussichtlich ist ein zeitlicher Abstand von Abfragen in der Größenordnung von wenigen Sekunden notwendig und sinnvoll.
4. **Telemetriedaten, die zwischen Fahrzeugen, Lieferanten von Subsystemen (Original Equipment Manufacturer, OEM) und Fahrzeugherstellern ausgetauscht werden**, können Entscheidungen des CPOs bei Einbindung des Ladevorgangs zur Netzstabilisierung oder Flexibilisierung erleichtern. Als Herausforderungen vorhersehbar sind die zum Großteil (noch) herstellerspezifischen und demnach nicht einheitlichen Standards sowie Bedenken betreffend Verletzungen der Sicherheit und der Privatsphäre.

Schwerpunkt der Studie ist demzufolge die konzeptuelle und technische Analyse der Sicherheit (siehe Definition im Kapitel 1.1), der Privatsphäre und der möglichen Gefährdung einer Fernsteuerung der Ladestation bei Kund_innen durch den Ladestationsbetreiber mittels OCPP. Die Studie schließt die Definition und Betrachtung realitätsnaher Anwendungsfälle anhand der aktuellen Implementierung der Ladeinfrastruktur in Österreich mit ein.

1.1 Definitionen: Komponenten, Systeme und Stakeholder

Für die Betrachtungen im Rahmen dieser Studie ist eine einheitliche Nomenklatur für Komponenten, Systeme und beteiligte Akteure notwendig. Auf die wesentlichen Begrifflichkeiten reduziert sind diese (unter Bezugnahme auf das Elektrizitätswirtschafts- und -organisationsgesetz 2010 – ElWOG [5] in der geltenden Fassung):

1. **Elektrofahrzeug** (kurz: **E-Fahrzeug**, **Fahrzeug**) wird definiert in §2 Abs2. Elektrisch betriebenes Fahrzeug, das an einem Ladepunkt geladen wird. In Sonderfällen kann der Energiefluss auch in die Gegenrichtung erfolgen (vom Fahrzeug zum Ladepunkt).

2. **Ladepunkt** (im OCPP-Standard: Charge Point, CP) definiert gemäß §2 Abs 3 von [5] als Schnittstelle, die das Laden eines Elektrofahrzeugs erlaubt. Ergänzend zu [5] ist bidirektionaler Fluss von Energie theoretisch möglich aber im Kontext dieser Studie nicht relevant.
3. **Ladestation** (**Charge Station**, **CS,** in OCPP 2.0.1): eine Aggregation mehrerer Ladepunkte. In OCPP erfolgt die Internet-Protokoll basierte Kommunikation zwischen Ladestationsbetreiber und Ladestationen. Über das Anwendungsprotokoll OCPP kann der bestimmte Ladepunkt adressiert werden. Im Kontext dieser Studie ist die Ladestation ein Gerät, das am Kund_innen (CSO) Standort (z.B. Haus, Wohnung, Firma) installiert ist. Die Ladestation ist am Energienetz angeschlossen und bezieht daraus die notwendige Energie, damit Kund_innen ihr Fahrzeug eigenbestimmt laden können. Die Ladestation verfügt über mindestens einen Ladepunkt mit den notwendigen Schnittstellen (standardisierte Stecker), um das Fahrzeug mittels Kabel anzuschließen und zu laden. Abhängig von dem Vorhandensein einer IT-Anbindung und Steuermöglichkeit unterscheidet man zwischen:
    a. **Offline-Ladestationen** sind für Ladestationsbetreiber nicht über Kommunikationsnetze erreichbar. Eine vertraglich zwischen Kund_innen und Verteilernetzanbieter vereinbarte Höchst-Ladeleistung ist für jeden Ladepunkt der Ladestation (oder die Ladestation insgesamt) konfiguriert und begrenzt die maximale Ladeleistung ladender Fahrzeuge. Eine Kommunikation zwischen Fahrzeug und Ladepunkt (typischerweise mittels Ladekabel) kann die effektive momentane Ladeleistung im Bereich zwischen 0 und dem festgelegten Maximalwert vereinbaren.
    b. Bei **Online-Ladestationen** ist eine zusätzliche Kontroll-Anbindung der Ladestation über Kommunikationsnetze vorhanden. Kund_innen oder andere Instanzen können mittels Software (z.B. Smartphone-Apps oder Web-Interfaces) die Ladeleistung der Ladepunkte bzw. Ladestation zusätzlich zum Fall (a) beeinflussen bzw. steuern.
4. **Kund_in** (alternativ: **Charging Station Owner**, **CSO**): ein Haushalt oder Unternehmen, der bzw. das als Endverbraucher_in Elektrofahrzeuge mittels einer eigenen, am festen Standort (z.B. Wohnort) installierten Ladestation lädt. Kund_innen verfügen über einen Zählpunkt und einen Netzanschluss, über welchen die Ladestation mit elektrischer Energie durch einen Stromlieferant beliefert wird.
5. **Verteilernetz** (**Energienetz**, Kurzform: **Netz**): die Infrastruktur und deren Management um Kund_innen an deren Standort (Haus, Wohnung, Firma) elektrische Energie bereitzustellen. Unter Netz wird in der Folge die Gesamtheit der Leitungsinfrastruktur aus Kupferleitungen, Spannungsumwandlern, Kontrollsystemen, Messeinrichtungen, usw., verstanden, die notwendig ist, um die Ladestation von Kund_innen mit Energie zu beliefern. Wenn nicht anders präzisiert, bezeichnet der Begriff Netz in dieser Studie das Verteilernetz der Ebene 5-7).
6. **Ladestationsbetreiber (Charge Point Operator**, **CPO)**: Ladestationsbetreiber bieten die Dienstleistung des Stromladens an. Sie sind kein Stromhändler oder Stromlieferant im Sinne des ElWOG.
7. **Ladestations-Managementsystem (Charge Point Management System, CPMS bis einschließlich OCPP 1.6 bzw. Charge Station Management System, CSMS ab OCPP 2.0.1)**: das System (Back-End) mit dessen Unterstützung CPOs die Ladestationen ansteuern und verwalten (d.h. Anbindung und Management).
8. **Stromlieferant**: gemäß §7 Abs 1 Ziffer 45: eine natürliche oder juristische Person oder eingetragene Personengesellschaft, die Elektrizität anderen natürlichen oder juristischen Personen zur Verfügung stellt. Soweit Energie von einer gemeinschaftlichen Erzeugungsanlage und innerhalb einer Bürgerenergiegemeinschaft sowie einer Erneuerbare-Energie-Gemeinschaft den Mitgliedern bzw. den teilnehmenden Berechtigten zur Verfügung gestellt wird, begründet dieser Vorgang keine Lieferanteneigenschaft;

9. **Verteilernetzbetreiber**: gemäß § 7 Abs 1 Ziffer 76. eine natürliche oder juristische Person oder eingetragene Personengesellschaft, die verantwortlich ist für den Betrieb, die Wartung sowie erforderlichenfalls den Ausbau des Verteilernetzes in einem bestimmten Gebiet und gegebenenfalls der Verbindungsleitungen zu anderen Netzen sowie für die Sicherstellung der langfristigen Fähigkeit des Netzes, eine angemessene Nachfrage nach Verteilung von Elektrizität zu befriedigen.
10. **Kommunikationsnetz** (IT, **IP-(Sub)Netz**): ein typischerweise paketorientiertes, auf dem Internet Protokoll (IP) basierendes und ans Internet angeschlossenes Datennetz, das abstrakte, bidirektionale Datenkommunikation zwischen unterschiedlichen Komponenten ermöglicht (z.B. Ladestation, PC, Server, Smartphone, Internet, Server, usw.). Das IP-Netz umfasst alle Ebenen, um Daten zwischen Endpunkten gemäß dem OSI-7-Schichten-Modell [6] zu vermitteln: beginnend mit dem physischen Übertragungsmedium und den Zugangstechnologien (kabelgebundene Technologien wie z.B. Ethernet, PLC, vDSL, Koaxialkabel, Glasfaser, bzw. Funktechnologien wie 2G/3G/4G Mobilfunk, WLAN, usw.) über Netzwerk- (IPv4 und IPv6) und Transport-Protokolle (TCP, UDP, SCTP, QUIC) bis zur Sicherheitsschicht und Anwendungseben (TLS, HTTP, und spezifischen Protokollen wie OCPP).
11. **Heim-Kommunikationsnetz** von Kund_innen (kurz: **Heimnetz, Local Area Network (LAN)**): es wird angenommen, dass Kund_innen über ein eigenes, von ihnen verwaltetes, lokales Kommunikationsnetz verfügen, mit Internetanbindung. Das lokale IP-Netz verwendet typischerweise den Ethernet-Standard, sowohl im drahtgebundenen Teil (IEEE 802.3) als auch im Funknetz (IEEE 802.11). Die Anbindung an das Internet erfolgt über ein Internet-Modem und – je nach Verfügbarkeit bzw. Wahl der Kund_innen – über kabelgebundene Zugangstechnologien wie vDSL, Koaxialkabel, oder Glasfaser oder über Mobilfunk (2G/3G/4G). Heute in Kommunikationsnetzen von Privathaushalten nicht üblich, jedoch technisch möglich und mit sicherheitstechnischen Vorteilen verbunden, ist eine Segmentierung des LAN in getrennte Subnetze mittels Virtual Local Area Networks (VLAN, IEEE 802.1Q) [7], zwischen denen auf höherer (IP-) Ebene geroutet werden muss. Damit ist eine sicherheitstechnisch effektive Trennung von Gerätekategorien bzw. -gruppen möglich.
12. Smart Charging: der Sammelbegriff für die intelligente Zusammenarbeit zwischen Auto, Ladesystem und Backend-Systeme, um Ladevorgänge zu überwachen, zu steuern und zu optimieren.
13. **Fernsteuerung** und -regelung (**Steuerung**): die Möglichkeit für den CPO, bei Bedarf (z.B. Engpass in der Energieversorgung, Überlast im Verteilernetz) mittels Datenkommunikation über das IP-Netz auf die im Besitz der Kund_innen befindliche Ladestation zuzugreifen und deren Ladeleistung zu steuern.
14. **Sicherheit**: umfasst im Rahmen dieser Studie die wesentlichen Elemente der Informations- bzw. Cybersicherheit, in der Fachliteratur meist referenziert als CIA-Triade (Confidentiality, Integrity, Availability) wie in [8] definiert. Folgende Sicherheitsziele sind dabei vorrangig und müssen gleichzeitig erfüllt sein:
    a. **Vertraulichkeit (Confidentiality):** Daten und ausgetauschte Nachrichten sollen ausschließlich den legitimen Sendern und Empfängern zugänglich sein. Ein typisches Beispiel für eine Maßnahme, um Vertraulichkeit sicherzustellen ist die Ende-zu-Ende Verschlüsselung mittels (starker) symmetrischer oder asymmetrischer Kryptographie.
    b. **Integrität (Integrity):** verhindert, dass unbefugte Dritte die am Kommunikationspfad zwischen Sender und Empfänger ausgetauschten Daten (unbemerkt von Sender, Empfänger, oder anderen Kontrollinstanzen) modifizieren. Ein typisches Beispiel einer kompromittierten Integrität wäre z.B. eine Veränderung von Werten oder Inhalten in einem Datenpaket durch einen Mittelsmann (sogenannten Man-in-the-Middle, MitM). Gängige Methoden zur Sicherstellung der Integrität in der

Netzwerkkommunikation sind z.B. Message Authentication Codes (MAC). Durch die Verwendung von digitalen Signaturen kann zusätzlich zur Integrität die Unleugbarkeit des Datenursprungs (non-repudiation) gewährleistet werden.

c. **Verfügbarkeit (Availability):** stellt sicher, dass die für die Erfüllung der Funktionen notwendigen Dienste (Services) verfügbar, d.h. für die legitimen Anwender nutzbar sind. Mit (Distributed) Denial-of-Services (DDoS) Angriffen versuchen beispielsweise Angreifer die Verfügbarkeit der DDoS-Ziele zu reduzieren.

15. **Cyber-physischer Angreifer (**kurz: **Angreifer):** bezeichnet eine Person, Gruppierung und/oder automatisierte Software (genauer: bösartige (Malicious) Software, Malware, wie z.B. Botnetze), die gezielt versucht, die ordnungsgemäße Funktion und/oder Sicherheit des Stromnetzes und/oder dessen Kontrollinstanzen zu beeinträchtigen. Typischerweise erfolgt ein Angriff aus der Entfernung, mit Unterstützung von IP-basierter Kommunikation, durch das Ausnutzen neuartiger oder bekannter Schwachstellen in Hardware, Software und/oder Kommunikation, bzw. durch Anwendung bekannter oder unbekannter Angriffsmethoden. Im Kontext der vorliegenden Studie verstehen wir unter **Angriff** eine Aktion von Angreifenden mit dem Ziel, entweder
    a. Den **Zugriff** bzw. die Fernsteuerung einer Ladestation im Eigentum der Kund_innen **durch den CPO zu stören oder zu unterbinden** (= Angriff auf die Verfügbarkeit), oder
    b. **Selber Zugriff auf die Fernsteuerung der Ladestation der Kund_innen zu erlangen (**= Angriff auf die Integrität oder Vertraulichkeit), oder
    c. Eine Kombination von (a) und (b) bei unterschiedlichen Kund_innen mit dem übergeordneten Ziel der Destabilisierung des Netzes.
16. **Sicherheitsmonitoring (mittels Intrusion Detection System (IDS))**: Unterschieden wird zwischen **proaktiver Sicherheit** (z.B. über Vermeiden/Eliminieren von Implementierungsfehlern in Software oder Hardware der eingesetzten Systeme, Nutzung von Sicherheitsprotokollen und Systemen zur Zugangskontrolle) und **reaktiver Sicherheit** (Erkennen von Verhaltensanomalien und Angriffen in laufenden Systemen). Das Sicherheitsmonitoring im Kommunikationsnetz ist eine reaktive Maßnahme. Die traditionell eingesetzten IDS arbeiten meist **signaturbasiert**: Angriffe werden aufgrund charakteristischer Bitmuster oder Verhaltensmuster bereits bekannter Angriffe (der sogenannten **Signatur**, typischerweise bereitgestellt durch Hersteller von Antivirensoftware) erkannt. Diese Erkennungsmethode ist sehr schnell und zuverlässig, hat aber einen entscheidenden Nachteil: sie erkennt ausschließlich bereits bekannte Angriffe. Neuere Systeme setzen daher auf **Anomalieerkennung und Maschinelles Lernen** (Machine Learning): IDS „lernen“ in einer ersten Phase ein „normales“ Verhalten des Kommunikationsnetzes, d.h. eine zeitliche Abfolge von Paketen, Paketgrößen, mögliche Sender und Empfänger, usw. Anschließend werden alle Abweichungen von diesem gelernten Muster als Anomalie gemeldet. Auf diese Weise können bisher unbekannte Angriffe erkannt werden – allerdings mit dem Risiko, dass viele Falschmeldungen (sogenannte „false positives“) untersucht werden müssen (wie z.B. ein Firmware-Update, das vorher nicht „gelernt“ wurde). Je regelmäßiger der Datenverkehr, desto erfolgsversprechender ist die Anomalieerkennung mit maschinellem Lernen in Kommunikationsnetzen.

1.2 Wissenschaftliche Beiträge dieser Studie

Die Studie analysiert die Sicherheit sowie mögliche Angriffsflächen und Gefährdungen der Privatsphäre im Falle der Fernsteuerung von privaten Ladestationen durch CPOs. Die Fernsteuerung der privaten Ladestationen durch CPOs stellt gegenüber bisherigen Architekturen einen Paradigmenwechsel dar, dessen Auswirkungen unklar sind und durch diese Studie qualitativ und quantitativ untersucht wird, insbesondere:

1. Eignung und Sicherheit von OCPP bei Fernsteuerung der Ladestationen privater Kund_innen
2. Mögliche Reaktionszeiten
3. Unterschiedliche Möglichkeiten der Anbindung über IT-Netze
4. Unterschiedliche Architekturen
5. Mögliche Verletzung der Privatsphäre der Kund_innen

Der verbleibende Teil der Studie ist strukturiert wie folgt: Kapitel 2 analysiert den Stand der Technik und fasst die Ergebnisse der durchgeführten Literaturrecherche bezüglich Standards, Protokolle und Sicherheit in der Ladeinfrastruktur zusammen. Kapitel 3 entwickelt das Systemmodell für die Sicherheitsbetrachtung der Studie, definiert Architekturen, Anwendungsfälle, notwendige Systemfunktionalitäten, Sicherheitsannahmen und unternimmt eine generische Sicherheitsanalyse der beteiligten Protokolle. Kapitel 4 untersucht die Machbarkeit der Ladestations-Steuerung anhand von Messungen der Reaktionszeiten in realen Mobilfunknetzen. Kapitel 5 enthält die detaillierte Sicherheitsanalyse für die in Kapitel 3 definierten Anwendungsfälle. Kapitel 6 bewertet die Anwendungsfälle bezüglich deren Eignung für die Steuerung von Ladestationen durch CPOs und fasst die wesentlichen Erkenntnisse in einer Übersicht der wesentlichen Anforderungen als Schlussfolgerung der Studie zusammen.

2 Stand der Technik

Das Laden von E-Fahrzeugen im öffentlichen Raum stellt ein komplexes System mit einer Vielzahl an Akteuren und Komponenten aus den Bereichen des Energie- sowie des IT-Systems dar, in dem eine Vielzahl an Protokollen zum Einsatz kommt, um an den zahlreichen Schnittstellen Kommunikation zu ermöglichen. Weiters ist das gesamte Ökosystem des Ladens von E-Fahrzeugen regulatorisch als auch technologisch (einschließlich relevanter Normen und Standards) weltweit in Entwicklung und (noch) nicht vereinheitlicht. Die Studie beschränkt sich daher in der Folge auf Protokolle und Strukturen, die im europäischen Raum (speziell DACH-Region) vorherrschend sind.

2.1 Protokolle und Standards

Aufbauend auf einer im Jahr 2020 veröffentlichte Analyse von verwendeten Protokollen für den Anwendungsbereich der E-Mobilität [9] gibt die Webseite der Forschungsstelle für Energiewirtschaft e. V. [10] einen Überblick und eine Beschreibung von Systemen und Protokollen beim Laden von E-Fahrzeugen, die aktuell eingesetzt werden bzw. in Entwicklung sind.

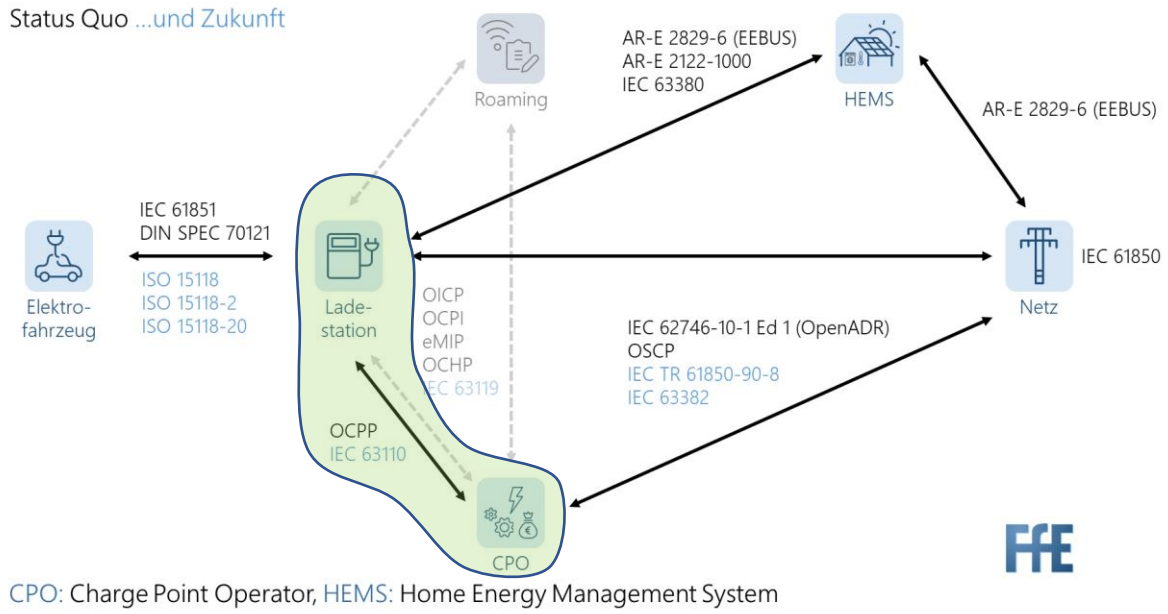

Abbildung 1: Normenlandschaft in der Ladeinfrastruktur aus Sicht der FfE (Abbildung mit freundlicher Genehmigung der Forschungsstelle für Energiewirtschaft e. V., FFE, [10], Abbildung 1).

Die beteiligten bzw. kommunizierenden Komponenten und Systeme in Abbildung 1 sind:

1. Elektrofahrzeug
2. Ladestation
3. Roaming-Hub
4. CPO
5. SmartHome Steuerung (HEMS)
6. Energienetz

In der Folge beschränkt sich die Studie ausschließlich auf die Betrachtung der (in Abbildung 1 grün hervorgehobene) Schnittstelle zwischen Ladestation und CPO, die für die geplante Ansteuerung von Ladestationen gegenständlich ist. Für die verbleibenden Protokolle und Schnittstellen wird auf die Zusammenfassung, Beschreibung, bzw. Querverweise in der Analyse der FfE [10] verwiesen.

Die Analyse der FfE [10] nennt zwei relevante Standards für die Kommunikation zwischen Ladestation und CPO: das von der OpenChargingAlliance (OCA) definierte Open Charge Point Protocol (OCPP, [4]) sowie das derzeit als potentieller Nachfolger von OCPP in Standardisierung durch die International Electrotechnical Commission (IEC) befindliche Protokoll IEC 63110.

2.1.1 IEC 63110

Der Standard IEC 63110 besteht aus drei Teilen:

1. IEC 63110-1 [11] für Definitionen und Anwendungsfälle
2. IEC 63110-2 [12] für Anforderungen und Protokolldefinition sowie
3. IEC 63110-3 [13] für Konformitätstests und -zertifizierungen

Die Verabschiedung des Standards – insbesondere des für die Implementierung relevanten Teils IEC 63110-2 – ist derzeit Schwerpunkt der Arbeitsgruppe TR69 der IEC. Geplant ist, dass IEC 63110 die bewährten funktionalen Gruppen (Primitive) des offenen OCPP-Standards anbietet, ohne jedoch abwärtskompatibel zu OCPP 2.0.1 zu sein [10]. Aufgrund der Ausgangslage sind die Zukunft und die Weiterentwicklung von IEC 63110 derzeit unklar: der aktuelle Stand der Standardisierung durch die IEC

ist nicht öffentlich zugänglich. Gemäß [10] arbeitet die IEC an einem Dokument, um den Übergang von OCPP 2.0.1 auf IEC 63110 zu ermöglichen.

Im Rahmen der verantwortlichen Gremien der EU (Standardisierungs-Subgruppe des Sustainable Transport Forum (STF)) spricht sich derzeit in [14] die Mehrheit der antwortenden Mitglieder für den Einsatz des offenen OCPP-Standards aus, anstatt auf IEC 63110 zu warten.

2.1.2 Open Charge Point Protocol: OCPP

Das derzeit dominante Protokoll für das Laden von E-Fahrzeugen, OCPP, definiert die Kommunikationsprotokolle zwischen Ladestation und einem zentralen Managementsystem (CPMS), dem Back-End der Ladestation. Das OCPP ermöglicht es dem CPMS, die Ladeinfrastruktur sowohl aus der Ferne zu überwachen und zu steuern als auch Funktionalitäten wie z.B. die Abrechnung zu verwalten. Dieses Protokoll ist in öffentlichen Ladestationen bzw. -netzwerken weit verbreitet und ermöglicht den Nutzer_innen, ihre E-Fahrzeuge an jeder beliebigen Station zu laden, die Teil des Netzwerks ist (Roaming, benötigt zusätzliche Protokolle wie z.B. das Open InterCharge Protocol, OICP). Da OCPP das in Österreich und der DACH-Region primär eingesetzte Protokoll für die Kommunikation zwischen Ladestation und CPMS ist, liegt der Studienschwerpunkt auf der Evaluierung der Sicherheit des OCPP-Standards.

OCPP besteht aus einer Reihe verschiedener Nachrichtentypen, welche die Kommunikation zwischen den Ladestationen und dem zentralen Managementsystem ermöglichen, wofür sich bereits eine Reihe an Nachrichtentypen etabliert hat, z.B.:

- "Authorize" für die Autorisierung und
- "StartTransaction" zum Starten eines Ladevorgangs
- "MeterValues“ zur Übermittlung von Zählerständen
- "StatusNotification" zur Übermittlung von Statusaktualisierungen (z.B. frei/belegt)

Zusätzlich zu diesen Kernnachrichtentypen enthält OCPP auch eine Reihe an Funktionen, die optional implementiert werden können. OCPP unterstützt weiters auch die Ferndiagnose, die es CPOs ermöglicht, Probleme an der Ladestation aus der Ferne zu diagnostizieren und zu beheben.

Der Einsatz von OCPP leistet somit einen wesentlichen Beitrag zur Benutzerfreundlichkeit, Effizienz und Sicherheit von Ladevorgängen. Durch die Implementierung von OCPP können CPOs ihre Ladeinfrastruktur einfacher verwalten und steuern und so die Zuverlässigkeit und den Komfort ihrer Systeme für die Nutzer_innen sicherstellen.

2.2 Zum aktuellen Stand der Forschung betreffend ”Sicherheit”

2.2.1 Generelle Einordnung: Publikationen zum Thema “Sicherheit”

Mit der gegenständlichen zentralen Forschungsfrage, der Sicherheit der Ansteuerung von Ladestationen bei Kund_innen durch CPOs, waren zum Zeitpunkt der Recherche keine praxisrelevanten Publikationen bekannt. Vorhandene Literatur betreffend ferngesteuertes Laden von E-Fahrzeugen und die Sicherheit der notwendigen Ladeinfrastruktur bzw. Protokolle ist tendenziell unspezifisch. Die Aussage trifft sowohl für die geringe Anzahl an Veröffentlichungen und Untersuchungen zu, als auch für die fehlenden Empfehlungen für bestimmte Protokollvarianten und Verfahren. Studien spiegeln mehrheitlich einen punktuellen Forschungsstand wider sowie erfolgreiche Angriffe, Erkenntnisse, Experimente und Sicherheitsanalysen. Weiters gibt es nur wenige Richtlinien, die Anforderungen an die Sicherheit von Ladeinfrastruktur selbst als auch an die praktische Systemarchitektur definieren. Dies gilt insbesondere hinsichtlich der Definition von Angriffsflächen und den Schäden für Kund_innen und Ladeinfrastruktur infolge möglicher Angriffe.

Im nachfolgenden Abschnitt findet sich ein Überblick über die aktuelle Forschung in den beiden stark verknüpften und teilweise sich überlappenden Bereichen Sicherheit von Ladeinfrastruktur und Sicherheit von Internet of Things (IoT)- bzw. Smart Home-Geräten. Gemeinsam ist den beiden Bereichen, dass aufgrund des Kostendrucks und der hohen Anzahl gleicher Geräte (Sensoren, Aktuatoren) in einem preissensitiven Marktsegment vor allem eingebettete Systeme (Embedded Devices) zum Einsatz kommen, die spezielle, hoch integrierte, günstige Hardware und dedizierte Software beinhalten. Der wesentliche Unterschied ist, dass Smart-Home Geräte typischerweise in Heim-IP-Netzen (WLANs) von Kund_innen betrieben werden. Sicherheitstechnisch bedingt der Kostendruck oftmals Nachlässigkeit der Hersteller (wie etwa unzureichende Verschlüsselung, fehlende Sicherheitsmaßnahmen, Default-Passwörter, fehlende Updates bei bekannten Sicherheitsmängeln, usw.)

2.2.2 Sicherheit der Ladeinfrastruktur

Der Aufbau der Ladeinfrastruktur wirft Fragen betreffend Sicherheit, potenzielle Schwachstellen und mögliche Folgen böswilliger Angriffe auf die Infrastruktur auf. Einige Studien versuchen, diese Bedenken auszuräumen. In [15] beispielsweise geben die Autoren einen umfassenden Überblick über verschiedene sicherheits- und datenschutzrelevante Themen, einschließlich der Risiken des Abflusses personenbezogener Daten, der Notwendigkeit der Einhaltung der CIA-Triade (siehe Definition in Kapitel 1.1) und der Auswirkungen auf sozialer, Cyber- und physischer Ebene. In [16] untersuchen die Autoren den Stand der Technik bei der Sicherung der Ladeinfrastruktur über mehrere Anbieter hinweg, heben aktuelle Herausforderungen hervor und schlagen potenzielle Verbesserungen für künftige Implementierungen vor. Schwerpunkt der Untersuchung liegt auf Kompromissen zwischen Sicherheit, Interoperabilität, Skalierbarkeit, Wirtschaftlichkeit und Energieeffizienz.

Weitere Studien dokumentieren erfolgreiche Angriffe auf die Ladeinfrastruktur. In [17] findet sich eine Auflistung der derzeit bekannten Angriffe, ihre Auswirkungen und mögliche Schutzmaßnahmen. Das Studienfazit lautet, dass **ein vollständiger Schutz gegen die derzeit beobachtbaren und bekannten Angriffe nicht möglich ist**, da die Protokolle ständig weiterentwickelt werden und es keine einheitlichen Standards gibt. Diese Angriffe können sich nicht nur auf die Kund_innen, sondern auch auf Betreiber auswirken, wie in [18] erörtert wird, das sich auf die Risiken und den Schutz aus der Sicht des IP-Netzes konzentriert. In der Studie finden sich Beispiele für Infiltrationsangriffe sowie Analysen der Auswirkungen der Position und Fähigkeiten des Angreifers und stellen fest, dass die jüngsten Verbesserungen der Ladeinfrastruktur in Bezug auf Flexibilität und Geschwindigkeit auch deren Anfälligkeit erhöhen.

Sicherheitsbedenken und Standards für die Kommunikation zwischen der Ladestation und dem Fahrzeug werden in [19] behandelt. Die Publikation weist darauf hin, dass eine z.B. für den Empfang von Kontrollnachrichten oder Firmware-Updates durch die Ladestation notwendige Internetverbindung zusätzliche Sicherheitsrisiken für das Kommunikationsnetz der Kund_innen schaffen kann. Die Sicherheit von Ladeinfrastrukturen auf Protokollebene wird in [20] untersucht. Die Studie enthält Empfehlungen für die Verwendung von OCPP, analysiert aktuelle Herausforderungen und stellt Beispiele für mögliche Angriffe auf das Protokoll vor. Eine umfassendere Untersuchung von OCPP und dessen sicherheitstechnischen Herausforderungen, einschließlich der in OCPP 2.0 eingeführten Erweiterungen und der vorgeschlagenen Verbesserungen, erfolgt in [21], wobei diese Studie auch ein breites Spektrum potenzieller Angriffe auf das Protokoll bei unsachgemäßer Verwendung enthält. Eine frühere Untersuchung potentieller Schwachstellen und Sicherheitslücken in OCPP ist in [22] zu finden.

Forscher von Kaspersky Labs identifizieren in [23] eine Reihe von Schwachstellen in Ladestationen, welche die Übertragung manipulierender Befehle ermöglicht. Konkret verschafften sie sich Zugang

zum lokalen IP-Netz, indem sie es mit einem Brute-Force-Verfahren durchsuchten, alle Geräte scannten und dann die mit dem öffentlichen IP-Netz verbundenen Ladestationen ohne jegliche Sicherheitsisolierung kontrollierten. Der Angriff beinhaltete die Änderung des Ladeprofils, d.h. die Reduzierung oder Erhöhung der Ladeleistung auf gefährliche Werte. Der Vollständigkeit halber muss angemerkt werden, dass der vorherige Angriff auch möglich gewesen wäre, wenn beispielsweise kompromittierbare IoT-Geräte ohne weitere Sicherungsmaßnahmen im Heimnetz von Kund_innen angeschlossen worden wären. Ohne eine gezielte Isolation aller vorhandenen (IoT-)Geräte (realisierbar beispielweise über deren Anschluss in getrennten IP-Subnetzen) durch Kund_innen hätte ein Zugriff eines Angreifers auf ein einziges der angeschlossenen IoT Geräte ausgereicht, um denselben Scanvorgang und alle nachfolgenden Manipulationen auszuführen.

Eine veröffentlichte Masterarbeit [24] implementiert eine abstrahierte Ladeinfrastruktur und untersucht deren Anfälligkeit auf bekannte Angriffe. Erwähnenswert ist, dass in der Arbeit Zertifikate nicht überprüft werden. Dadurch sind einige Angriff möglich, die normalerweise, durch ordnungsgemäße Abfrage der Gültigkeit der Zertifikate, erkennbar wären.

Eine andere Angriffskategorie zielt auf persönliche Informationen und die Privatsphäre ab. Einige Hersteller (z. B. Tesla und Audi) verlangen vom Benutzer, dass er anderen Anwendungen auf dem Gerät, wie z. B. dem Kalender, Zugriff auf die mit der Ladestation verbundenen Anwendungen gewährt. Bei Kompromittierung der Ladestation (z.B. mittels modifizierter Firmware) kann dieser Zugriff eskalieren und zu Zwischenfällen führen, wie z. B. der Extraktion privater Benutzerdaten und, im schlimmsten Fall, der Verbreitung von Malware, abhängig von der genehmigten Zugriffsebene.

Zusammenfassend gibt es einige Forschungsarbeiten, die sich mit Sicherheitsfragen in der Ladeinfrastruktur befassen. Die Gesamtarchitektur und Implementierung von Lösungen bleibt aufgrund der kontinuierlichen Entwicklung in Frage kommender Standards und Systeme derzeit noch großteils den Entscheidungen der CPOs bzw. Betreiber überlassen. Ähnliche Herausforderung stellen sich im Bereich IoT und SmartHome Sicherheit. Der folgende Abschnitt betrachtet Publikationen und Forschungsergebnisse in den letztgenannten Bereichen, um mögliche Gemeinsamkeiten mit angeschlossenen und vom CPO gesteuerten Ladestellen von Kund_innen zu evaluieren.

2.2.3 Sicherheit von IoT und Smart-Home

Die fortschreitende Verbreitung und der Einsatz von IoT-Geräten durchdringen zunehmend alle Bereiche des täglichen Lebens. Sensoren und Aktuatoren im öffentlichen und privaten Bereich liefern Daten und steuern Geräte, die von intelligenten Heizungen bis zu PV-Wechselrichtern, Beschattungssystemen, oder Multimedia-Systemen reichen. Gemeinsam ist den IoT-Geräten die Notwendigkeit der Vernetzung bei gleichzeitigem hohen Kostendruck, der die Gefahr birgt, Sicherheit zugunsten von Funktionalität zu vernachlässigen. Die Integration dieser Geräte in Heimnetze von Anwendern birgt daher auch Risiken, die analysiert, bewertet und durch geeignete Schutzmaßnahmen minimiert werden müssen. In [25] untersuchen die Autoren beispielsweise die Schwachstellen von kostengünstigen IoT-Geräten für Verbraucher. Deren unaufwändige Kompromittierung ermöglicht potentiellen Angreifern Zugang zum gesamten Heimnetzwerk von Kund_innen. Die Autoren schlagen konkrete Lösungen und Umgehungsmöglichkeiten vor, um diese Probleme zu beheben. In ähnlicher Weise präsentiert [26] eine umfassende Sammlung von Schwachstellen, kategorisiert Geräte, Zugriffsarten sowie Angriffe und liefert Statistiken zu den verursachten Schäden, ohne sich jedoch mit Abwehr- oder Schutzmaßnahmen zu befassen.

Während, wie in Kapitel 1.1 unter Sicherheitsmonitoring definiert, die **proaktiven Sicherungsmaßnahmen** die Sicherheit von IoT und SmartHome Geräten zu verbessern versuchen, kann angesichts der Schwachstellen und des Kostendrucks eine Kompromittierung nie ausgeschlossen werden. Empfehlenswert und notwendig ist daher eine zweite Komponente, die **reaktive Sicherheit**,

deren wesentlicher Bestandteil die Erkennung solcher Angriffe oder deren erfolgreiche Kompromittierungen ist. In [27] geben die Autoren einen Überblick über den aktuellen Stand der Technik bei der Erkennung von IoT-bezogenen Bedrohungen, einschließlich der traditionellen signaturbasierten Erkennung und modernerer, auf maschinellem Lernen basierender Ansätze (siehe Definition Sicherheitsmonitoring in Kapitel 1.1). In [28] wird auch der potenzielle Einsatz von maschinellem Lernen zur Erkennung von Angriffen erörtert, wobei Beispiele dafür gegeben werden, wie verschiedene Kategorien von Angriffen durch Methoden wie Link-State-Monitoring und Beobachtung des Gerätezustands angegangen werden können.

In einem umfassenden Überblick gehen die Autoren von [29] auf die theoretischen Aspekte und die aktuelle Forschung ein, die zur Sicherung von IoT-Infrastrukturen und zur Entwicklung von Standards durchgeführt wird. Die Autoren untersuchen auch die für die Funktionalität oder die Kommunikation verwendeten Protokolle, die mehrere Schichten von der physikalischen bis zur Anwendungsschicht abdecken. In der Studie wird betont, dass die proaktive Sicherheit äußerst wichtig ist. Jedoch räumen die Autoren ein, dass Schwachstellen in IoT-Systemen schon immer vorhanden waren und auch in Zukunft vorhanden sein werden – daraus ergibt sich die Notwendigkeit einer reaktiven Sicherheitskomponente zur Erkennung von Angriffen und dem Auslösen von Alarmen bzw. Gegenmaßnahmen.

Smart-Home-Geräte sind in den meisten Fällen **IoT-Geräte**, die als Besonderheit (a) direkt oder über Gateways Verbindung zum lokalen Kommunikationsnetz von Kund_innen haben und (b) gleichzeitig über das Internet oder eigene Kommunikationskanäle (z.B. Mobilfunk) mit den Servern und Clouds der SmartHome Gerätebetreiber kommunizieren. Diese Anbindung macht aus SmartHome Geräte potentielle Einfallstore für Angreifer und schafft eigene Risiken, insbesondere in Umgebungen, in denen sensible Geräte angeschlossen sind. Zu diesem Thema gibt es bereits eine Vielzahl an Publikationen, was zum Teil auf die rasche Zunahme der Nutzung von Smart-Home-Geräten zurückzuführen ist, insbesondere derjenigen, die von Amazon, Google und Apple angeboten werden. Mit der Verbreitung von E-Fahrzeugen ist die Anzahl an privaten Ladestationen, die mit dem jeweiligen Heimnetzwerk verbunden sind auch signifikant angestiegen. Dieser Umstand bringt erhebliche Risiken – spezifisch für SmartHome Geräte – mit sich, die im Folgenden erörtert werden.

In [30] identifizieren die Autoren eine Reihe von Risiken, die bei der Verwendung von Smart-Home-Systemen mit mehreren Geräten zur Steuerung von Versorgungseinrichtungen auftreten. Sie erörtern Herausforderungen bezüglich der Zugangskontrolle, Zugangserweiterung und unbefugten Weitergabe persönlicher Daten. In ähnlicher Weise macht [31] auf die Risiken bei der Installation von Smart-Home-Geräten aufmerksam und verweist auf die große Zahl von Herstellern, die eine Vielzahl von Geräten mit unterschiedlichen Protokollen und Kommunikationstechnologien und manchmal sogar ungetesteten proprietären Anwendungen produzieren. Die Autoren argumentieren, dass es aufgrund der Heterogenität der Geräte nicht möglich ist, alle Schwachstellen und Risiken zu untersuchen und zu erkennen, und schlagen stattdessen vor, dass sich die Branche an Standards und Mindestsicherheitsanforderungen halten sollte. In [32] wird der Fokus eingegrenzt, indem eine Liste von persönlichen Informationen erstellt wird, die von persönlichen Geräten nach einem böswilligen Zugriff auf Anwendungen von Drittanbietern durchsickern können. Die Studie enthält auch Beispiele für 10 mögliche Angriffe und 15 Risiken und deren jeweilige Folgen.

[33] geht noch weiter und analysiert Smartphone-Apps, die Smart-Home-Geräte steuern, und zeigt auf, wie diese Apps Zugriff auf Telefonressourcen anfordern und damit Möglichkeiten für Datenlecks und die Verbreitung von Malware bieten. Sowohl [34] als auch [35] bieten umfassende Übersichten über die Risiken, Empfehlungen, Probleme und Herausforderungen im Zusammenhang mit vernetzten Smart Homes. Diese Studien geben Entwicklern auch Ratschläge, wie sie Angriffsflächen in ihren

Systemen und Anwendungen minimieren können, und diskutieren die möglichen Folgen für das Stromnetz, wenn sich Malware aufgrund von Schwachstellen verbreitet.

Zusammenfassend kann festgehalten werden, dass die in Abschnitt 2.2.2 und 2.2.3 dargelegte Sichtung der vorhandenen Literatur betreffend Sicherheit von Ladeinfrastrukturen für E-Fahrzeuge sowie Sicherheit von Smart-Home-Systemen und IoT-Geräten den Schluss auf wesentliche konzeptuelle Schwachstellen, Angriffsmöglichkeiten und Risiken für diese Gerätekategorien ermöglicht.

2.2.4 Die Forschungsergebnisse im Überblick: Identifikation von Schwachstellen und Gefährdungen

Die Autoren dieser Studie haben aus den vorhandenen Publikationen die **folgenden generischen Ursachen bzw. Risiken für Sicherheit, Angriffe und Gefährdung der Privatsphäre in Kommunikationsnetzen aufgrund des Einsatzes von Smart-Home-Geräten einschließlich Ladestationen identifiziert**:

1. **Vielzahl an Geräten und Herstellern**: Private Haushalte verwenden in der Regel eine Vielzahl an Smart-Home-Geräten bzw. Komponenten (PCs, Laptops, Smartphones, SmartTV, Wärmepumpe, PV-Wechselrichter, Waschmaschine) von unterschiedlichen Herstellern, die typischerweise ohne spezifische Sicherheitsmaßnahmen (z.B. zusätzliche Subnetze, VLANs, Firewalls, Zugriffsregeln) mit dem LAN (lokalen Kommunikationsnetz) der Kund_innen verbunden werden und untereinander als auch mit beliebigen Servern im Internet kommunizieren. Das führt zu einer heterogenen Vielzahl an Geräten und Komponenten, die gleichzeitig bzw. gemeinsam zum Einsatz kommen.
2. **Vielzahl an Protokollen und unklare Standardisierung**: Es findet sich eine Vielzahl von implementierten Protokollen im Einsatz, mit zum Teil mehrfachen, redundanten Implementierungen im gleichen Produkt oder nicht ausreichend spezifischen Standards (mit Auslegungsmöglichkeiten). Insbesondere wenn verwendete Standards noch nicht “ausgereift” sind ist es in der Praxis oftmals der Fall, dass Hersteller „Zwischenlösungen“ implementieren. D. h. da Version 1 des Standards funktionale Defizite aufweist, Version 2 des Standards aber (noch) nicht implementiert ist, werden einzelne, ausgewählte Features von Version 2 in Version 1 implementiert. Typische Bezeichnungen für derartige “Zwischenlösungen” bzw. Hybride sind z.B. „xyz ready“, z.B. „Smart Grid Ready“. Typischerweise ist es allerdings so, dass der genaue Umfang, welche Teile einer Spezifikation im Rahmen des Hybrids implementiert wurden, nicht transparent und demnach nicht nachvollziehbar ist. Folglich sind derartige Hybride in Bezug auf die Sicherheit zu hinterfragen bzw. ist von deren Einsatz ohne explizite Sicherheitsprüfung abzuraten.
3. **Redundante Kommunikationspfade**: Es ist nicht unüblich, dass Hersteller im selben Gerät mehrere Kommunikationstechnologien gleichzeitig implementieren, z.B. WLAN und Mobilfunk und/oder Bluetooth. Daraus resultieren unklare, redundante Kommunikationspfade. Bei unsauberer Implementierung können dadurch – unbeabsichtigt oder bewusst – niederschwellige Einfallsmöglichkeiten für Angreifer entstehen bzw. geschaffen werden.
4. **Hoher Kostendruck**: Die Integration von Sicherheit (Software und Hardware) wird aufgrund des Kostendrucks zugunsten von Funktionalität vernachlässigt oder die Hardware ist in Bezug auf Rechenleistung oder Speicher zu gering dimensioniert, um langfristig verlässliche Sicherheit zu implementieren. Die Konsequenz daraus ist, dass z.B. das zum Zeitpunkt der Herstellung gerade noch ausreichende Sicherheitsprotokoll (hypothetische Schlüssellänge z.B. 2048 Bit) wenige Jahre später nicht auf die mittlerweile notwendige 4096-Bit Schlüssellänge aktualisiert werden kann und folglich die Kommunikation ggf. kompromittierbar ist.

5. **Komplexe Konfigurationsanforderungen**: Kund_innen sind mit der Konfiguration der Geräte und Sicherheitsmaßnahmen überfordert. Alternativ konfigurieren manche Hersteller Standard-Passwörter ab Werk, die für alle Geräte einer Serie gleich und für die Inbetriebnahme der Geräte notwendig sind. Diese Default-Konfigurationen bieten allerdings keine ausreichende Sicherheit, da ein Angreifer bei Bekanntwerden des Standard-Passworts das Gerät im Zuge der Inbetriebnahme kompromittieren kann.
6. **Fehlende Updates**: Ein nicht vernetztes Gerät wäre am sichersten vor Angriffen über das Kommunikationsnetz. Das Einspielen von notwendigen bzw. empfohlenen Firmware- und Software-Updates der Geräte ist jedoch oft nur mit Internet-Anbindung möglich und birgt ggf. zusätzliche Gefahren (z.B. unsichere Verbindungen, nicht signierte Software, usw.).
7. **Unbekannte Daten und Zugriff auf Privatsphäre**: Aus Kund_innen-Sicht sind Umfang und Inhalt gespeicherter Kund_innendaten bei Ladevorgängen oder bei Zugriff des CPOs auf die Ladestation schwer nachzuvollziehen. Die unklare Datenlage betrifft sowohl a) übertragene bzw. extern, beim Hersteller gespeicherte kund_innenbezogene Daten, als auch b) den Speicherort der Daten (z.B. Cloud außerhalb von EU, demzufolge unklare Anwendbarkeit von Anforderungen der Datenschutz-Grundverordnung (DSGVO) [36]).

Es verbleiben viele offene Fragen und potenzielle Bereiche für zukünftige Forschung, einschließlich der Entwicklung von Standards und Best Practices, um die stetig sich entwickelnden Herausforderungen bei der Sicherung dieser Systeme und dem Schutz vor oder der Erkennung von Angriffen zu bewältigen. Diese Studie konzentriert sich im Folgenden auf die Sicherung von Systemen, bei denen die Komponenten der Ladestationen bei Endkund_innen installiert sind.

2.3 Architektur und Sicherheitsmaßnahmen der Ladeinfrastruktur in Österreich

Aufbauend auf der Literaturrecherche erfolgt eine Beschreibung der aktuell vorherrschenden Strukturen und damit einhergehenden Sicherheitsmaßnahmen:

1. CPOs betreiben derzeit selbst Ladestationen und solche im Kund_innenauftrag. Die Ladestationen sind mit dem CPMS (Back-End) des CPO permanent verbunden. Der CPO implementiert eine Abrechnung der Ladevorgänge auf Basis der Authentifizierung der Kund_innen (Ladekarten, Smartphone Apps) einschließlich Roaming-Ladevorgänge. Dabei kann – wenn auch nicht ganz trennscharf - unterscheiden werden zwischen:
    a) Öffentlicher Ladeinfrastruktur: im öffentlichen Raum diskriminierungsfrei zugängliche Ladestationen z.B. entlang von Straßen
    b) Halb-öffentliche Ladeinfrastruktur: die Ladestationen werden von einem Standortpartner betrieben, ggf. durch den CPO betreut, es bestehen aber mitunter Einschränkungen der öffentlichen Zugänglichkeit durch zusätzliche Anforderungen im Bereich der Authentifizierung, Nutzung und Bezahlung (z.B. Kundenparkplätze von Supermärkten mit eingeschränkten Öffnungszeiten, Tiefgarage eines Hotels/Einkaufszentrums, Ladestation eines Hotels).
    c) Private Ladestationen: Ladestationen, die Kund_innen in der Regel an ihrem Wohnort für das Laden von E-Fahrzeugen errichtet haben.
2. Die Kommunikation mit Ladestationen des CPOs erfolgt durch Mobilfunktechnologie (2G/3G/4G) sowie andere kabellose oder auch kabelgebundene Kommunikationstechnologien (z.B. Ethernet mittels WLAN, LAN im Netz von Kund_innen). Es werden sicherheitstechnische Vorkehrungen getroffen (z.B. private APNs bei Mobilfunkbetreibern, Binden von SIM-Karten an Mobile Modems (IMEI Lock), usw.). Auf höheren Protokollebenen wird TLS-Verschlüsselung (noch) nicht

flächendeckend eingesetzt. Drei Gründe sind für die die zum Teil noch fehlende TLS-Verschlüsselung maßgeblich:

a) Zu geringe Rechenleistung der Ladestation (aufgrund des bereits angesprochenen Kostendrucks, bzw. des Alters und fehlender Upgrade-Möglichkeit der Ladestation).
b) Zu lange mögliche Kommunikations-Laufzeiten bei 2G (aufgrund der höheren Datenmenge und der Notwendigkeit des Aufbaus gesicherter TLS-Verbindungen – siehe Kapitel 3.5.2 und 4.4.3).
c) Fehlende (sichere) out-of-band Zeitsynchronisation der Ladestationen und mögliche Herausforderungen im Zusammenhang mit kurzlebigen Server-Zertifikaten – siehe Kapitel 5.4.1.4.

3. Es bestehen derzeit noch keine Anforderungen an private Ladestationen hinsichtlich ihrer Kommunikationsfähigkeit und Steuerbarkeit. Der Zeitpunkt, die Leistung und Dauer des Ladevorgangs durch die Kund_innen ist weder festgelegt, noch kann der CPO oder eine externe Instanz darauf Einfluss nehmen, d.h. Leistung steuern oder ihn unterbinden. Durch Gleichzeitigkeit der Ladevorgänge (z.B. in den kritischen Abendstunden zwischen 17 und 19 Uhr) entsteht die Gefahr der Überlastung der Verteilernetze. Aufgrund der TOR Verteilernetzanschluss in der geltenden Fassung ([37], Kapitel 5.9.2) besteht für Ladestationen über 3.68 kVA bei Inbetriebnahme ab 1.1.2025 eine Verpflichtung für eine bidirektionale digitale Steuerschnittstelle. Zusammenfassend kann über private Ladestationen zum jetzigen Zeitpunkt festgehalten werden:
   a) Sie befinden sich im Privateigentum und sind autark, für CPOs nicht steuerbar
   b) Sie sind nicht notwendigerweise vernetzt (ab 1.1.2025 gemäß TOR Verteilernetzanschluss jedoch verpflichtende bidirektionale Kommunikations-Schnittstelle)
   c) Falls vernetzt, besteht ggf. ein „versteckter Pfad“ für Kontrolle durch Ladestations-Hersteller mittels App-Interfaces (analog zu anderen Geräten wie Wechselrichtern oder SmartHome Geräten): Bei Anbindung der Anlage über ein Kommunikationsnetz hat der Hersteller über Monitoring-Funktionen ggf. Zugriff auf die Ladestationen. Diese Anbindung kann für Updates und Kontrolle durch den Hersteller verwendet werden unter Umgehung der Zuständigkeit von Kund_innen und vorhandener Sicherheitsmaßnahmen. Als ein warnendes Beispiel gilt die Kompromittierung russischer Ladestationen durch eine ukrainische Softwarefirma im Frühjahr 2022 [38].
   d) CPOs und Verteilernetzbetreiber haben derzeit aufgrund fehlender Kommunikation mit Ladestationen bei Kund_innen keine Information über die jeweils momentan bezogene Leistung – auch nicht grobgranular. Im Rahmen von Smart Metering ist derzeit eine Auflösung von maximal alle 15 Minuten möglich ([39], [40]), wonach am Netzübergabepunkt hinsichtlich der jeweils momentan bezogenen Leistung “Blindheit” besteht.
4. Die Sicherheit privater Ladestationen wird durch die Notwendigkeit der Steuerung durch eine zentrale Managementeinheit (CPMS) einerseits reduziert, da *nicht vernetzte* Ladestationen *nicht* durch Dritte steuerbar und daher (vermeintlich) sicherer sind. Andererseits sind (a) die Notwendigkeit der Software-Updates von Ladestationen sowie (b) das Bereitstellen von lokalen Access Points durch Ladestationen für die Konfiguration zwei schwerwiegende Argumente, die für die Vernetzung von (privaten) Ladestationen sprechen. Zumal eine Absicherung der genannten Vorgänge (Update, Konfiguration) ohnehin notwendig ist, um den Missbrauch dieser Schnittstellen durch Angreifer oder andere Geräte in der Umgebung zu verhindern. **Standardisierte, kontrollierte, und sichere Schnittstellen für CPOs ermöglichen eine niederschwellige Laststeuerung und sind das Mittel der Wahl für die Vernetzung von Ladestationen.**
5. Für die Kommunikationsnetz-Anbindung privater Ladestationen zum Zwecke der Steuerung durch CPOs gibt es keine vorhandenen, standardisierten Vorgaben oder Implementierungen. Es kann angenommen werden, dass CPOs für die Kommunikation entweder (a) vorhandene Internet-

Anbindungen der Kund_innen, also Kabel, vDSL, Glasfaser oder Mobilfunk, oder (b) dedizierte Mobilfunk-Verbindungen bzw. -Modems des CPOs in der Ladestation verwenden werden.

6. OCPP ist das derzeit von CPOs am häufigsten eingesetzte und europaweit bevorzugte Protokoll für die Steuerung von Ladestationen [14].

3 Systemmodell für Sicherheitsbetrachtungen

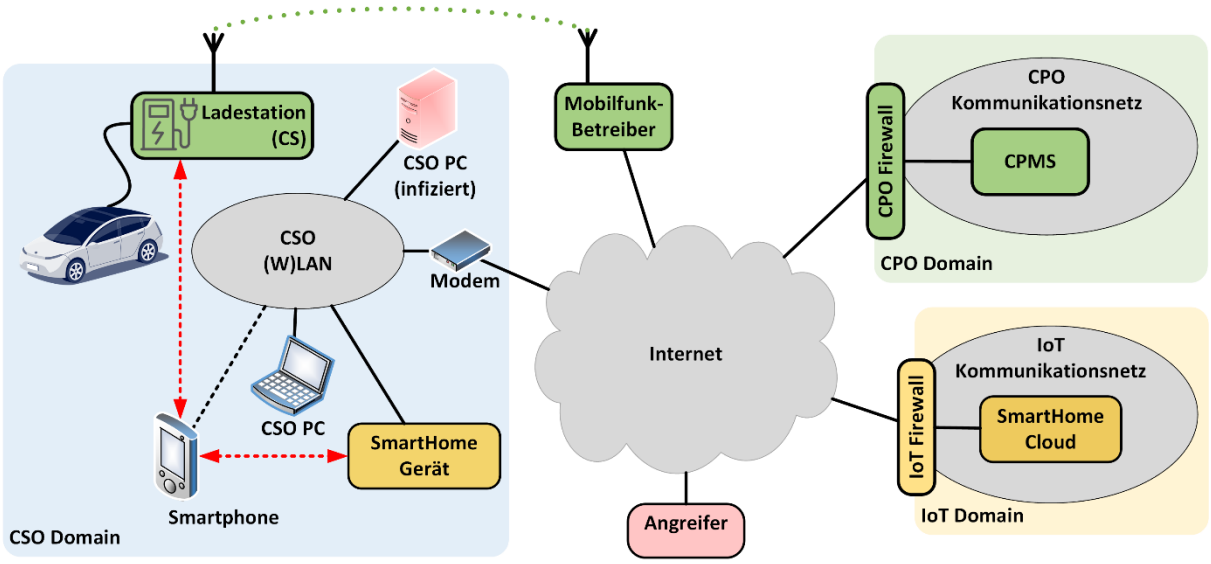

Abbildung 2: Generisches Modell für die Steuerung von Ladeinfrastruktur durch CPO: Architektur, Komponenten, Kommunikationspfade und Akteure.

Abbildung 2 zeigt eine generische Architektur, die im weiteren Verlauf für die Analyse der Sicherheit OCPP-basierter Steuerung von Kund_innen-Ladeinfrastruktur durch CPOs verwendet wird. Wesentlich sind die betrachteten Domänen, Akteure, Architekturen und Komponenten sowie mögliche Kommunikationspfade. Im linken Teil der Abbildung befindet sich der Zuständigkeitsbereich/ die Verwaltungsdomäne der Kund_innen (CSO), in der Mitte das öffentliche Internet und im rechten Teil der Zuständigkeitsbereich/ die Verwaltungsdomäne des CPO bzw. anderer beteiligter Akteure. Die Verwaltungsdomäne der Kund_innen betrifft primär Privathaushalte, ist jedoch gleichermaßen auf andere Anwendungsfälle wie Hotels, Restaurants oder KMUs anwendbar.

Zentrale Funktion, die in dieser Studie betrachtet wird, ist die kontrollierte Leistungsreduktion privater Ladestationen durch das CPMS des CPOs im Anlassfall. Die notwendige Kommunikation soll über IP-Kommunikationspfade erfolgen, die teilweise über das öffentliche Internet verlaufen (je nach betrachtetem Fall über Mobilfunk oder/und über das Heimnetz der Kund_innen). Die Details werden in den kommenden Unterkapiteln erörtert.

3.1 Architektur, Systeme, Netze: Modell als Ausgangsbasis für Sicherheitsanalyse

In einem ersten Schritt werden die Annahmen bezüglich der betrachteten Infrastrukturen konkretisiert, um darauf aufbauend die Anwendungsfälle zu definieren.

3.1.1 Domänen

Das abstrahierte Modell in Abbildung 2 trennt die Zuständigkeitsbereiche/ Verwaltungsdomänen, um die Grundlagen für eine spätere Diskussion der Privatsphäre bzw. Sicherheit und möglicher Angriffsvektoren zu schaffen. Komponenten und Netze innerhalb einer Verwaltungsdomäne werden von den jeweils Zuständigen administriert und konfiguriert. Unterschieden wird dabei zwischen:

1. Kund_innendomäne (Charging Station Owner, CSO): links in Abbildung 2 – umfasst ein Kommunikationsnetz und die angeschlossenen Geräte entsprechend dem typischen Setup von Kund_innen.
2. Charge Point Operator Domäne (CPO): rechts oben in Abbildung 2.
3. Domänen anderer Beteiligter – z.B. diverser SmartHome-Hersteller (IoT) – rechts unten in Abbildung 2 beispielhaft als Gegenstelle eines SmartHome-Geräts im LAN von Kund_innen dargestellt.
4. Angreiferdomäne: mittig unten in Abbildung 2. Angreifer werden üblicherweise einen Standort im öffentlichen Internet bevorzugen, der sie bei potentieller Erkennung vor unmittelbarem Zugriff der zuständigen Exekutive von Kund_innen und CPOs schützt. In einigen Fällen kann der Angreifer auch auf (z.B. durch Malware oder Botnetze) kompromittierte Komponenten in den IP-Netzen von Kund_innen oder vom CPO zugreifen bzw. diese Komponenten kontrollieren.

Die folgenden Unterkapitel besprechen die Eigenheiten der Kommunikationsnetze und Systeme von Kund_innen, CPO und Angreifer im Detail.

3.1.2 Varianten der Kommunikationsnetze im Rahmen der betrachteten Domänen

Für die Sicherheitsanalyse relevant sind bestimmte Eigenschaften bzw. Annahmen und Anforderungen der IT-Netze der Kund_innen, des CPOs sowie des öffentlichen Internets.

1. **Heimnetz (Kommunikationsnetz von Kund_innen):** Angenommen wird, dass gemäß heutigem Stand der Technik (siehe Kapitel 2.3) ein lokales Kommunikationsnetz (WLAN und/oder LAN) alle Geräte einer Kund_in in einem einzigen IP-Subnetz verbindet, ohne Möglichkeit der Segmentierung und Trennung auf Protokollebene (z.B. VLAN, siehe Kapitel 1.1). Sicherheitstechnisch von hoher Relevanz ist das mögliche Vorhandensein von proprietären Zugangsmethoden, -netzen und -protokollen von SmartHome-Geräten, die damit Sicherheitsmaßnahmen im (W)LAN umgehen können. Beispiele sind Kommunikationsprotokolle wie z.B. Bluetooth, Zigbee oder dedizierte WLAN APs, die von einigen Geräten wie z.B. Wechselrichter, Ladestationen, usw. für direkten Kund_innenzugriff angeboten werden. In Abbildung 2 greift beispielsweise ein im WLAN angemeldetes Smartphone mittels direkter Kommunikation (rot strichliert dargestellt) auf Ladestation und SmartHome-Gerät zu und umgeht damit mögliche Sicherheitsmaßnahmen im LAN oder WLAN. Ausgegangen wird von den folgenden, wesentlichen Eigenschaften der Kund_innen-LANs:
    a. Ein LAN ohne Segmentierung: Angeschlossene Geräte in der Kund_innendomäne können mit beliebigen anderen Geräten der Kund_innen sowie mit Geräten im öffentlichen Internet ungehindert und i.A. unerkannt kommunizieren.
    b. Internet-Zugang: Internet-Zugang der Kund_innen wird durch ein Modem realisiert, das als externe Zugangstechnologie Kabel, xDSL, Mobilfunk oder in seltenen Fällen Glasfaser verwenden kann.
    c. IP-Adressierung: IP-Adressvergabe für die Geräte im Netz erfolgt standardmäßig durch das Access-Modem (z.B. VSDL- oder Kabelmodem). Geräte im LAN und WLAN der Kund_innen erhalten typischerweise Adressen aus einem privaten IPv4 Adressbereich sowie optional global gültige IPv6 Adressen (in Österreich seit ca. Frühjahr 2020 bei einigen Telekom-Betreibern Standard). Das Modem implementiert die Network Address Translation (NAT) Technologie, um Kommunikation von Kund_innengeräten mit privaten IPv4-Adressen nach extern (ins Internet) auf eine durch den Telekombetreiber zugewiesene öffentliche IPv4-Adresse abzubilden.

d. Duale Zugangspfade: Relevant für die Sicherheitsanalyse ist, dass einige Geräte im Netz mittels mehrerer unterschiedlichen Schnittstellen bzw. Technologien Zugang zum öffentlichen Internet (oder zu privaten Kommunikationsnetzen von Diensteanbietern) haben. In Abbildung 2 hat z.B. die Ladestation eine Schnittstelle im LAN der Kund_innen und eine unabhängige Anbindung über das Mobilfunkmodem mit SIM-Karte des CPOs. Gleiches gilt möglicherweise für SmartHome-Geräte und Komponenten anderer Kategorien. Die Gefahr dieser Topologie ist die Möglichkeit für externe Angreifer, diese dual angebundenen Geräte von Kund_innen als sogenannte Jump-Hosts für das schwer zu identifizierende Ausspähen und Angreifen von anderen Kund_innengeräten zu missbrauchen.
e. Überwachung und Schutz: Standardmäßig wird das Internet-Modem von Kund_innen durch den Kommunikationsnetzanbieter (A1, Magenta, usw.) bereitgestellt. Letzterer aktualisiert bei Vorhandensein bzw. Notwendigkeit die Firmware des Internet-Modems. Die Firewall des Internet-Modems ist typischerweise rudimentär und nicht gewartet, überwacht bestenfalls Kommunikation zwischen dem LAN und dem Internet, nicht aber Kommunikation innerhalb der Komponenten des (W)LAN. Einen minimalen Schutz vor dem IP-Zugriff von außerhalb auf Geräte innerhalb des Heimnetzes bietet die interne Verwendung von privaten Adressbereichen für die Geräte sowie das typische IPv4 NAT durch das Internet-Modem. Mit der gleichzeitigen Verteilung von IPv6 Adressen entfällt jedoch diese Sicherheit – d.h. zusätzliche Firewall-Sperren am Internet-Modem sind dringend zu empfehlen.

2. **Kommunikationsnetz des CPOs:** Annahme der Studie ist, dass das Kommunikationsnetz des CPOs aufgrund gesetzlicher Anforderungen (NIS/NIS2, kritische Infrastruktur) gemäß dem aktuellen Stand der Technik geschützt ist. Im Detail:
    a. IP-Subnetze: Die Kommunikationsnetze des CPOs sind nach Verwendungszweck segmentiert (Subnetze mit Trennung durch VLANs und Routing). Nur Geräte derselben Kategorie bzw. Klasse können ungehindert miteinander kommunizieren.
    b. Internet-Zugang: Redundante, breitbandige, überwachte Internet-Zugänge sind Standard.
    c. IP-Adressierung: Streng administriertes Kommunikationsnetz mit fester Zuweisung von (privaten oder öffentlichen) IPv4- und (eventuell öffentlichen) IPv6-Adressen zu Geräten sowie Überwachung und Warnung im Fall unberechtigten Zugriffs (z.B. unbekannte IP-Adresse im Kommunikationsnetz).
    d. Verbot dualer Zugangspfade: für Betreiber kritischer Infrastrukturen sind vernetzte Geräte, die die Überwachung durch die Firewall (z.B. mittels eines Mobilfunkmodems) umgehen, eine permanente Gefährdung. Vorschriften der CPOs bzw. Betreiber sollten derartige Lösungen verlässlich verhindern.
    e. Firewall (evtl. unterstützt durch IDS): Redundante, leistungsfähige, gewartete (evtl. selbstlernende) Firewalls und IDS trennen und schützen das Kommunikationsnetz des CPOs vor Angriffen und Zugriffen aus dem öffentlichen Internet. Die Kommunikation zwischen internen und externen Geräten wird großteils mitgeloggt und dieses Monitoring kann zu Alarmen führen.
3. **Kommunikationsnetz des Angreifers:** Im Verlauf der Studie werden mehrere Optionen der Vernetzung bzw. Positionierung eines potentiellen Angreifers analysiert. Wesentlich ist, dass der Angreifer einen "sicheren" Ort wählt und ggf. über kompromittierte oder infizierte Komponenten privilegierten Zugriff auf die Kommunikation zwischen den Komponenten von Kund_innen und CPO erhält. Folgende mögliche Standorte des Angreifers kommen in Frage:
    a. Internet, außerhalb des Kommunikationspfades Kund_innen-CPO
    b. Internet, nur mitlesend am Kommunikationspfad Kund_innen-CPO

c. Internet, lesender und schreibender Mittelsmann (Man-in-the-middle, MitM) am Kommunikationspfad Kund_innen-CPO
d. LAN von Kund_innen
e. Kommunikationsnetz des CPOs
f. Ladestation von Kund_innen
g. CPMS des CPOs

3.2 Anwendungsfälle

Betrachtet werden **vier Anwendungsfälle (Use Cases), wobei bei Anwendungsfall 2 zwei Untervarianten unterschieden werden**. Der erste Fall, Anwendungsfall 0, repräsentiert den zum überwiegenden Teil Ist-Stand bei privaten Ladestationen (offline Ladestation, d.h. ohne Kommunikationsnetz-Anbindung, demnach auch nicht vernetzt) und wird demnach nur der Vollständigkeit halber als Anwendungsfall 0 erwähnt. Für den Rest dieser Studie sind ausschließlich die folgenden Anwendungsfälle 1, 2-1, 2-2 und 3 von Bedeutung.

3.2.1 Anwendungsfall 0: Offline Ladestation

Dieser in Abbildung 3 dargestellte Use Case, dass die Ladestation gar nicht über ein Kommunikationsnetz erreichbar ist, repräsentiert den derzeit noch häufigsten Status. Dies schließt allerdings nicht aus, dass möglicherweise lokale Zugriffsmöglichkeiten über andere Protokolle existieren, um das Einbinden der Ladestation in eine etwaige SmartHome Umgebung zu erleichtern (z.B. Modbus/TCP o.ä.). Jedoch hat der CPO jedenfalls keinerlei Zugriffsmöglichkeit auf die Steuerung der Ladestation - weder über das Kommunikationsnetz der Kund_innen, noch über andere Schnittstellen. Eine Steuerung oder ein Monitoring der Ladestation ist demzufolge für den CPO nicht möglich.

Aufgrund der Vorgaben in der aktuellen TOR Verteilernetzanschluss ([37], Kapitel 5.9.2) ist ab 1.1.2024 allerdings nur mehr Anschluss von Ladestationen mit bidirektionaler Steuerung zulässig, wonach der Use Case 0 zunehmend an Bedeutung verlieren wird.

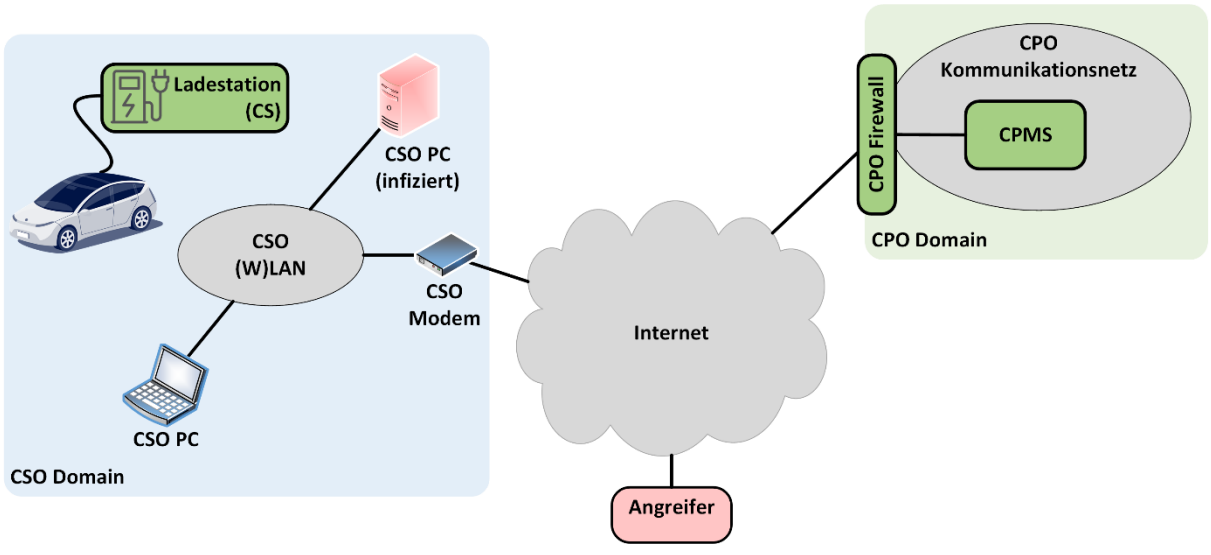

Abbildung 3: Anwendungsfall 0: Autarke Ladestation, keinerlei Zugriff des CPO auf Kund_innen-Ladestation vorhanden (Ausgangslage dieser Studie).

3.2.2 Anwendungsfall 1: Zugriff auf die Ladestation ausschließlich über Mobilfunk

Der CPO greift im Anwendungsfall 1 ausschließlich über Mobilfunk auf die Ladestation (mittels SIM-Karte in der Ladestation) von Kund_innen zu, was zur Folge hat, dass die **Kund_innen auch keinen Direktzugriff** über LAN oder WLAN auf ihre Ladestation haben. Wenn Kund_innen die Ladestation steuern oder konfigurieren möchten, müssen sie z.B. über ein Cloud- oder WebService des CPOs gehen (derzeit schon Status quo bei z.B. PV-Wechselrichtern).

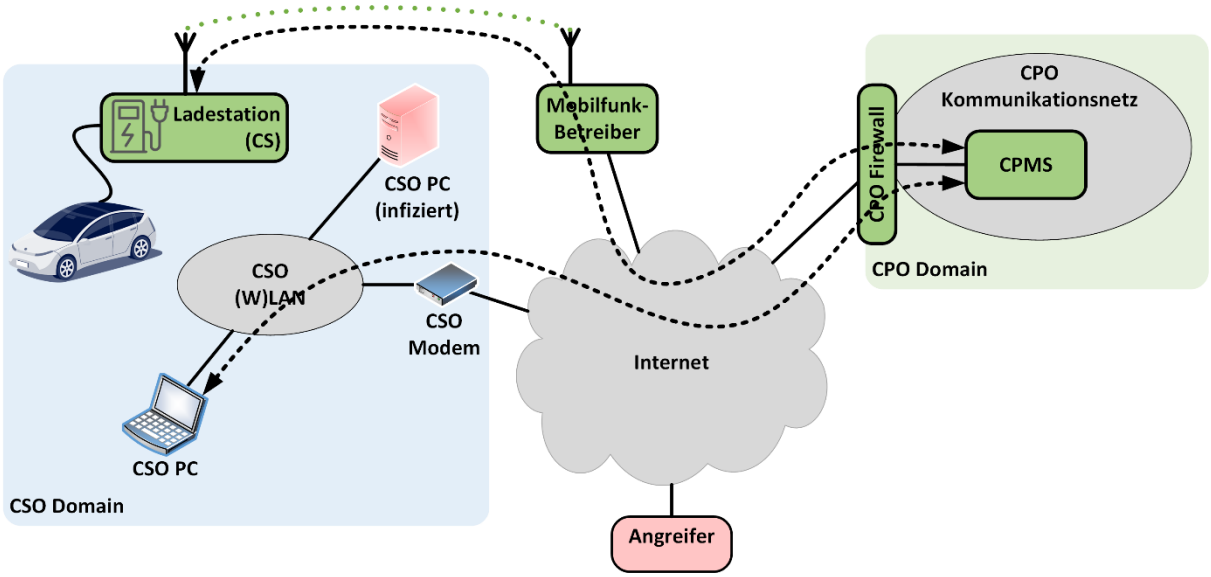

Abbildung 4: Anwendungsfall 1: Zugriff des CPO auf Kund_innen-Ladestation ausschließlich über Mobilfunk. Keine Anbindung der Ladestation ans lokale Kommunikationsnetz von Kund_innen.

3.2.3 Anwendungsfall 2-1 und 2-2: Zugriff auf die Ladestation über das Kommunikationsnetz der Kund_innen

In Anwendungsfall 2 hat der CPO über das Heim-Kommunikationsnetz und die Infrastruktur von Kund_innen Zugriff auf die Ladestation. D.h. die Kund_innen haben eine Heimnetz-Anbindung über vDSL, Kabel oder Mobilfunk und die Ladestation ist im LAN/WLAN der Kund_innen angemeldet.

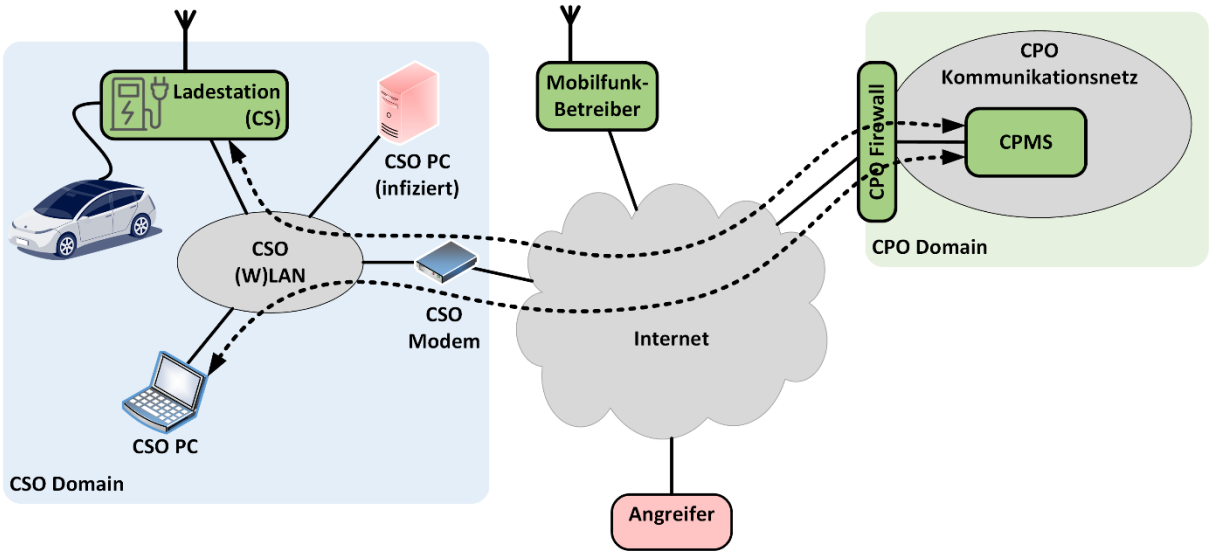

Abbildung 5: Anwendungsfall 2-1: Zugriff des CPO auf Kund_innen-Ladestation ausschließlich über Internet-Anbindung der Kund_innen. Kein Mobilfunk-Zugriff des CPOs auf die Ladestation von Kund_innen. Kund_innen haben keinen lokalen Zugriff auf Ladestation.

Unterschieden werden bei Anwendungsfall 2 die zwei Unterfälle:

Im Anwendungsfall 2-1 in Abbildung 5 erfolgt der Zugriff auf die Ladestation durch die Kund_innen ausschließlich über Schnittstellen (APIs) des CPO auf die Ladestation zu. Die Kund_innen selbst können nicht direkt auf die Ladestation zugreifen, obwohl diese in ihrem eigenen (W)LAN angemeldet ist.

Im Anwendungsfall 2-2 in Abbildung 6 können Kund_innen hingegen direkt, lokal, auf die Ladestation zugreifen (z.B. über eine App oder das Web-Interface der Ladestation).

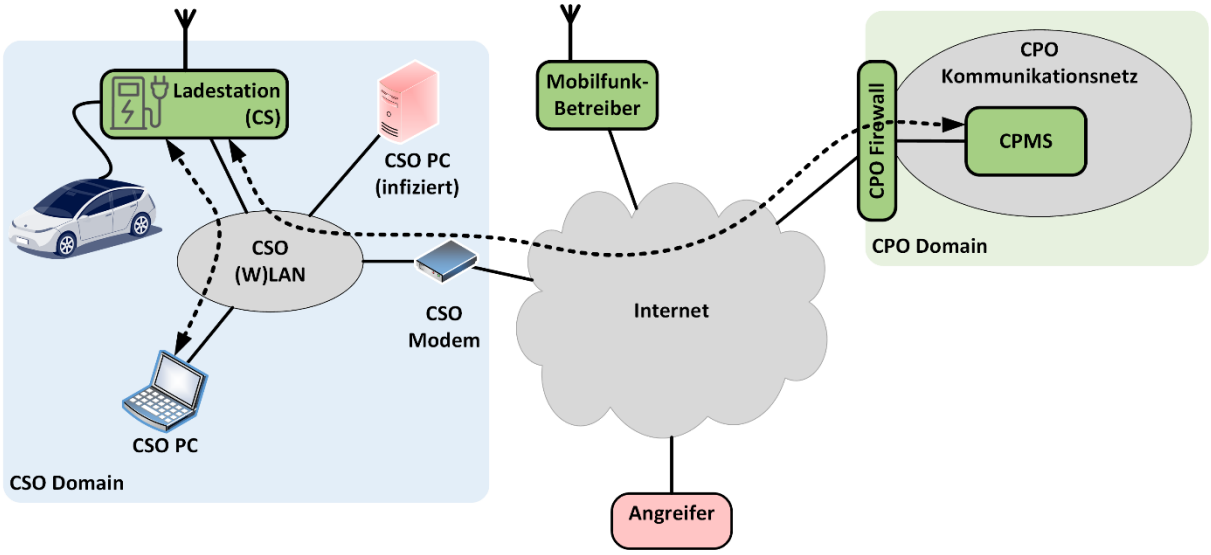

Abbildung 6: Anwendungsfall 2-2: Zugriff des CPOs auf Kund_innen-Ladestation ausschließlich über Internet-Anbindung von Kund_innen. Keine Mobilfunk-Zugriff des CPOs auf die Ladestation von Kund_innen. Kund_innen greifen lokal auf die Ladestation zu.

3.2.4 Anwendungsfall 3: Zugriff auf die Ladestation über Mobilfunk und Kommunikationsnetz der Kund_innen

Der Anwendungsfall 3 stellt eine Kombination von Anwendungsfall 1 und 2 dar, wonach der CPO über Mobilfunk und Kund_innen (W)LAN auf die Ladestation Zugriff hat und die Kund_innen auch einen direkten Zugriff auf die Ladestationen lokal über (W)LAN haben.

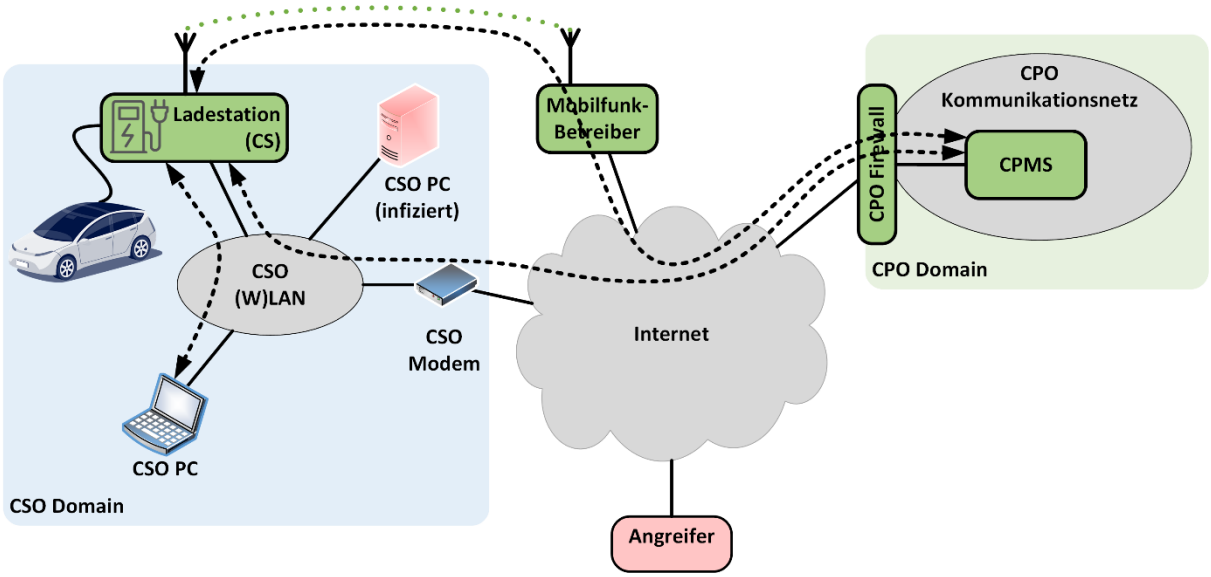

Abbildung 7: Anwendungsfall 3: Zugriff des CPO auf Kund_innen-Ladestation über Internet-Anbindung der Kund_innen und/oder über Mobilfunk.

Mit Hinblick auf die Position des Angreifers werden für die Anwendungsfälle 1, 2-1, 2-2 und 3 jeweils folgende Fälle unterschieden:

1. Angreifer im Internet
2. Angreifer im LAN der Kund_innen oder in der IT-Infrastruktur des CPOs
3. Angreifer hat Ladestation infiziert
4. Angreifer hat das CPMS des CSO infiziert

Bei den Angriffsfällen 3 und 4 bestehen nur wenige bis keine Möglichkeiten zur Erkennung und Abwehr. Eine theoretische Option für die Erkennung wäre eine holistische Analyse, über Kombination von zusätzlichen, potentiell nicht kompromittierten Sensoren wie beispielsweise die abgenommene Energiemenge und dem momentanen Energiefluss im Smart Meter der Kund_innen. Da die Angriffsfälle 3 und 4 realistisch nicht abwehrbar sind, werden in weiterer Folge nur die Angriffsfälle 1 und 2 betrachtet.

3.3 Notwendige Systemfunktionalitäten

Eine Technologie zur Ladestationsansteuerung muss aus Sicht der Kund_innen und des CPO einige Funktionalitäten erfüllen, um die Flexibilisierungspotenziale des Ladens von E-Fahrzeugen optimal nutzen zu können.

3.3.1 Notwendige Funktionalitäten für die Kund_innen

Die offensichtliche Funktionalität, die für Kund_innen gewährleistet sein muss, ist das Laden des E-Fahrzeugs, sodass es einsatzfähig ist, wenn es benötigt wird. Diese scheinbar selbstverständliche Anforderung ist allerdings keinesfalls trivial, sobald ein großer Anteil des Individualverkehrs durch Elektromobilität erbracht wird. Eine intelligente Steuerung von größeren Lasten im Verteilernetz ist somit im Interesse der Allgemeinheit. Für die Kund_innen selbst ist es erstrebenswert, entsprechende Möglichkeiten zu haben, ihren Bedarf an Ladeenergie auch kostentechnisch optimieren zu können.

Letztlich sollte für Kund_innen auch die Möglichkeit gegeben sein auf ein Interface zuzugreifen, das Monitoring- oder Steuerungsmöglichkeiten der eigenen Ladestation bereithält. Dieser Zugriff muss

nicht zwangsläufig direkt erfolgen, sondern kann über eine Cloudlösung des CPOs (Anwendungsfall 1) realisiert werden.

3.3.2 Notwendige Funktionalitäten für den CPO

Die Steuerung der Ladeleistung von E-Fahrzeugen durch einen CPO bietet die Möglichkeit im Fall von Engpässen im Verteilernetz reagieren zu können und andererseits, um vorhandene Flexibilitätspotenziale für das Energiesystem nutzen zu können Die relevante notwendige Funktionalität für den CPO ist daher die Steuerung der Ladeleistung an Kund_innen-Ladestationen. Eine zur Netzstabilisierung notwendige Reduktion der Ladeleistung im Falle von Frequenzabfällen stellt allerdings nennenswerte Anforderungen an die Kommunikation mit der Ladeinfrastruktur, da hier eine Reaktion innerhalb von Sekunden notwendig ist. Der CPO muss daher mit der Ladestation kommunizieren können und auch eine Schnittstelle für Verteilernetzbetreiber anbieten, um im Anlassfall Ladestationen herabregeln zu können. Schlussendlich muss sichergestellt werden, dass die Latenz dieser Steuerung den Anforderungen für die Stabilisierung des Netzbetriebs genügt.

3.3.3 Interessenskonflikte

Es ist anzumerken, dass Interessen zur Ausnutzung der oben genannten Funktionalitäten von Kund_innen und CPO sich nicht notwendigerweise überlappen. Erlauben Kund_innen dem CPO die Reduktion der Ladeleistung ihrer Ladestationen zwecks Netzstabilisierung oder Flexibilisierung, so haben sie keine unmittelbaren Vorteile hiervon. Die Reduktion der Ladeleistung kann in beiden Fällen nachteilig für Kund_innen sein, da möglicherweise Fahrzeuge nicht vollständig geladen sind, wenn sie benötigt werden. Der für CPOs notwendige Steuerungszugriff auf Ladestationen der Kund_innen muss sorgfältig abgesichert werden um potentiellen Angreifern keine zusätzlichen Angriffsflächen zu bieten.

Finanzielle Anreize sind eine grundlegende Möglichkeit für den CPO um bei Steuerung von Ladestationen von Kund_innen die eigenen Interessen mit denen der Kund_innen in Einklang zu bringen. Wird Kund_innen eine Flatrate für den Opt-In in eine Laststeuerung geboten, ist für Sicherheitsbetrachtungen auch relevant, dass Kund_innen die Laststeuerung gezielt umgehen könnten, um bei gleichzeitigem Bezug der finanziellen Vorteile keine Nachteile für die eigene Ladefunktionalität zu haben.

3.3.4 Sicherheitsaspekte und Privatsphäre

Sowohl für Kund_innen als auch für CPOs müssen jederzeit Datensicherheit, Datenschutz und (vor allem für Kund_innen) Privatsphäre gewährleistet sein. Für Kund_innen kann dieser Aspekt kritisch sein, da bei Mitbenutzung der Internetanbindung von Kund_innen für die Steuerung der Ladestation ein durch den CPO kontrolliertes Gerät auf das Kommunikationsnetz (WLAN, LAN) der Kund_innen zugreifen kann. Neben dem Aspekt, dass der CPO in diesem Fall grundsätzlich Zugriff auf das Kommunikationsnetz der Kund_innen hat, ist zu berücksichtigen, dass Kund_innen möglicherweise den direkten Einfluss auf eine sichere Konfiguration der Ladestation verlieren.

3.4 Sicherheitsannahmen und -gefährdungen

Die sicherheitstechnischen Anforderungen und Auswirkungen müssen in der Folge im Detail analysiert werden. Ausgangspunkt und Vergleichsgegenstand ist die Annahme einer zurzeit (wenn überhaupt) nur lokal durch Kund_innen steuerbaren Ladestation. D.h. die Ladestation ist nicht oder nur für Kund_innen lokal, aus dem eigenen Heimnetz (LAN/WLAN), mittels Datenkommunikation ansprechbar, jedenfalls nicht für den CPO).

Es gilt nun in den weiteren Schritten die zusätzlichen Angriffspotentiale zu identifizieren, die sich aufgrund der Möglichkeit der Steuerung privater Ladestationen durch deren CPO mittels Datenkommunikation entsteht.

3.4.1 Gefährdung der Sicherheit

Die wesentliche Voraussetzung, damit CPOs Ladestationen bei Kund_innen steuern können, ist notwendigerweise ein sicherer Fernzugriff des CPOs auf die Ladestation mittels Datenkommunikation. Hierbei müssen die in Kapitel 1.1 erwähnten beiden Randbedingungen erfüllt sein: (1) der CPO muss im Bedarfsfall (d.h. jederzeit) steuern können und (2) ausschließlich er soll steuern dürfen, d.h. für die Steuerung autorisiert sein. Diese Randbedingungen bedeuten sicherheitstechnisch äquivalent (unter Verwendung der in Kapitel 1.1 unter Punkt 14 detaillierten CIA-Triade in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit), dass gemäß (1) mögliche Angreifer weder den Steuerungszugriff des CPO einschränken bzw. gemäß (2) mögliche Angreifer keinesfalls selber Ladestationen steuern können dürfen.

Einleitend wurde in bereits in Kapitel 1 auf die stark steigenden Zahlen von Elektrofahrzeugen in Österreich hingewiesen. Dieser Erfolg erzwingt einen starken Ausbau der Ladeinfrastruktur und die Verfügbarkeit einer hohen Anzahl baugleicher, kommunikationstechnisch angebundener Ladestationen im Feld (bei Kund_innen). Aus Sicht potentieller Angreifer sind das hohe steuerbare Gesamtleistungen: eine Schwachstelle in der Implementierung der Ladestations-Software kann Angreifern die Möglichkeit eröffnen um viele Ladestationen zu kompromittieren. Der Missbrauch potentieller Sicherheitslücken in der Steuerung von Ladestationen bedroht folglich nicht nur die Ladeinfrastruktur als solche, sondern auch die Stabilität des gesamten Energienetzes. Aus Sicht des Angreifers notwendig für eine Destabilisierung des Energienetzes ist koordiniertes Fehlverhalten einer großen Anzahl von Ladestationen in einer Netzregion. Gefährdend für die Netzstabilität ist deswegen vor allem die Gruppe der cyber-physischen Angriffe, die Angreifern einen mit wenig Risiko behafteten und wenig aufwändigen Zugriff und Angriff (a) aus der Ferne (b) innerhalb kurzer Zeit und (c) auf eine große Anzahl von Ladestationen ermöglichen.

Besonderes Augenmerk benötigen Ladestationen (oder IoT-Komponenten), die über zwei unterschiedliche Kommunikationsschnittstellen verfügen. Gemäß Anwendungsfall 3 (Kapitel 3.2.4) sind das Ladestationen, die sowohl über das Heimnetz der Kund_innen angebunden sind, als auch über dedizierte, zusätzliche Kommunikations-Schnittstellen, die von den Kund_innen nicht überwacht werden können. Ein Beispiel wäre z.B. eine Ladestation mit eigenem Mobilfunkmodem und SIM-Karte mit Anbindung zum CPO. Auf diese Weise verfügt die Ladestation über einen Rückkanal, der beispielsweise Erkenntnisse aus dem Heimnetz der Kund_innen an den CPO melden kann, ohne Kund_innen eine Möglichkeit für Erkennung oder Unterbindung zu bieten (beispielsweise über ein IDS oder Monitoring-Tool im LAN). Weitere Betrachtungen sind Teil des folgenden Unterkapitels betreffend die Privatsphäre.

3.4.2 Gefährdung der Privatsphäre

Die Fernsteuerung der Ladestation eröffnet sowohl für den CPO als auch für mögliche Angreifer die Möglichkeit, die Privatsphäre der Kund_innen zu verletzen. Dieser Fall ist insbesondere gegeben, wenn die Ladestation mit dem lokalen Kommunikationsnetz (Heimnetz, LAN, WLAN) der Kund_innen verbunden ist und CPO oder Angreifer Vollzugriff auf die Ladestation haben. Der Vollständigkeit halber anzumerken ist, dass diese Aussage für jedes SmartHome-Gerät zutrifft, das mit dem LAN der Kund_innen verbunden ist. Die Bedrohung der Privatsphäre ist also architekturell bedingt, weder spezifisch für OCPP als Steuerungsprotokoll noch für den steuernden Zugriff des CPOs auf Ladestationen.

In den vorhergehenden Kapiteln (u.a. 1.1 (11), 2.2.2, und 3.1.2) wurde festgehalten, dass eine Ladestation durch Sicherheitsmaßnahmen wie IP-Subnetting und VLANs komplett von den anderen Komponenten im Heimnetz von Kund_innen abgeschirmt werden kann bzw. auch soll. Diese zusätzliche Sicherheitsmaßnahme ist jedoch bei Privatkund_innen derzeit unüblich: als Default-Einstellung der Internet-Provider wird ein einziges LAN bzw. IP-Subnetz verwendet, in dem alle Geräte angeschlossen sind. In diesem Fall bedeutet ein Vollzugriff auf die Ladestation, dass jedes Gerät des Heimnetzes von der Ladestation aus direkt erreichbar ist. Wenn CPO oder Angreifer die Ladestation als sogenannten Jump-Host verwenden, können diese unter anderem:

1. Den Datenverkehr des Heimnetzes (teilweise, je nach Konfiguration) abhören und aufzeichnen, einschließlich möglicher, die Privatsphäre gefährdenden Inhalte (sofern nicht Ende-zu-Ende verschlüsselt). Ein beispielhafter Angriff ist die Aufzeichnung von IP-Datenpaketen unverschlüsselter oder schwach verschlüsselter Kommunikation anderer Geräte im WLAN um z.B. unverschlüsselte Passwörter auszuspähen (=Angriff auf die Vertraulichkeit der Daten).
2. Aktiv nach anderen, im Heimnetz angeschlossenen oder aus dem Heimnetz erreichbaren Komponenten suchen. Ein Beispiel ist das aktive Scannen von IP-Adressbereichen des WLAN um andere im WLAN vorhandene Geräte zu finden. Anschließend kann die MAC-Adresse dieser gefundenen Geräte Rückschluss auf den Hersteller und evtl. Gerätetyp liefern.
3. Sobald Geräte gefunden wurden, können Angreifer aktiv nach möglichen Sicherheitslücken dieser erreichbaren Komponenten suchen und das Ausnützen dieser Sicherheitslücken starten. Beispielsweise möglich ist die Identifikation bestimmter Gerätetypen und -Serien anhand der vom Hersteller zugewiesenen MAC-Adressbereiche. Anschließend kann der Angreifer ein Port-Scanning starten, um installierte und aktive Dienste auf den Geräten zu identifizieren, sowie ggf. Software-Versionen herauszufinden. Auf dieser Basis folgt das gezielte Ausnutzen bekannter und noch nicht behobener Schwachstellen (z.B. anhand von Datenbanken, CVE-Listen und Informationen des Herstellers zu Fehlerbehebungen in bestimmten Firmwareversionen).
4. Das zeitliche Verhalten der gefundenen Komponenten anhand des Datenverkehrs untersuchen und daraus Privatsphäre und Sicherheit gefährdende Schlüsse ziehen. Ein typisches Beispiel wäre das Aufzeichnen der Öffnungs- oder Schließbefehle für Rollos, Türen, Fenster, Multimediaanlagen, usw. um auf (Nicht)Anwesenheit der Kund_innen zu schließen.
5. Den vorhandenen, legitimen Datenverkehr des Heimnetzes verwenden, um die eigene (bösartige, aktive) Kommunikation dem vorhandenen Verkehr anzugleichen und zu versuchen, auf diese Weise evtl. vorhandenen IDS oder Monitor-Tools zu umgehen. Entsprechende Methoden fallen unter die Begriffe Netzwerk-Steganographie, bzw. verdeckte Kommunikation (covert channel, subliminal channel).

3.4.3 Sicherheit und Privatsphäre

Aus Sicht von Angreifern ist die Infektion eines ersten Systems im LAN von Kund_innen der sprichwörtliche „Fuß in der Türe“ – auch bekannt als „Patient Zero“ – und der wichtigste Schritt bei der Kompromittierung eines Netzwerks. Um Privatsphäre und Sicherheit von Kund_innen zu schützen, ist das technische Ziel der Studie die Identifikation von Möglichkeiten und Sicherheitsmängeln in der Fernsteuerung der Ladestationen, mit denen:

5. **Ein Angreifer die notwendige Steuerung von privaten Ladestationen durch den CPO erschweren, stören oder unterbinden kann**
6. **Ein Angreifer aufgrund von Sicherheitslücken Ladestationen übernehmen und regeln kann**
7. **Ein Angreifer die Punkte (1) und (2) für eine große Anzahl von Ladestationen erreicht.**

8. **Ein Fernzugriff auf die Ladestation durch Angreifer oder CPO die Privatsphäre der Kund_innen gefährdet.**

3.4.4 Annahmen bezüglich der Möglichkeiten und Fähigkeiten von Angreifern

Die Komplexität der Ladeinfrastruktur, die Vielzahl von involvierten Akteuren, Systemen, Technologien und Protokollen macht eine Sicherheitsanalyse herausfordernd.

Grundsätzlich wird festgehalten bzw. angenommen, dass es kein sicheres System gibt. Die Frage ist nicht ob, sondern wann und wer, in welcher Komponente, mit welchem Ziel Schwachstellen entdeckt und ggf. ausnutzt. Eine Sicherheitsanalyse ist demzufolge notwendigerweise mit spezifischen Annahmen verknüpft. Wesentlich dabei ist, dass bewährte Sicherheits-Architekturen, -Konzepte und -Protokolle, idealerweise aus den Bereichen der Kommunikation in kritischen Infrastrukturen, als Referenz herangezogen werden.

Um die folgende, konkrete Sicherheitsanalyse der Ladeinfrastruktur realistisch zu gestalten, müssen die Sicherheitsannahmen der Studie genauso wie Möglichkeiten und Fähigkeiten potentieller Angreifer möglichst generisch identifiziert und protokolliert werden. Die folgenden, ausführlichen Listen sollen es ermöglichen bzw. erleichtern, später gezielte Updates dieser Studie durchzuführen bzw. einzelne Annahmen zu hinterfragen und zu ändern.

Annahmen: Die Studie setzt voraus:

1. Alle betrachteten Systeme (PCs, Netzwerkkomponenten, Ladestationen, Server, usw.) sind gemäß derzeitigem Stand der Technik abgesichert. Diese Annahme schließt das Vorhandensein von dem Angreifer exklusiv bekannten, punktuell erfolgreichen Exploits (Zero-Days) NICHT aus (siehe auch Positivliste Angreifer für weitere Detaillierung). Insbesondere gilt jedoch:
    a. Es gibt keine bekannten, offensichtlichen Sicherheitslücken, die dem Angreifer die Übernahme aller betrachteten Komponenten bzw. Komponentenkategorien ermöglichen.
    b. Insbesondere geht die Studie davon aus, dass es Angreifern NICHT gelingt, Hardware, Software oder Firmware-Image für alle Ladestationen eines Herstellers zu kompromittieren (z.B. über erfolgreiche Supply-Chain Angriffe).
    c. Die Firmware von Ladestationen ist auf dem neuesten Stand. Firmware-Updates werden nach Möglichkeit und Verfügbarkeit sofort eingespielt.
    d. Es gibt keine bekannterweise gefährdeten Dienste, Services, offene Ports und ähnliche Sicherheitslücken auf den relevanten Komponenten (Ladestation, CPO).
    e. Komponenten haben eine lokale Firewall, die Angriffe gemäß (d) erfolgreich unterbindet.
2. Die sicherheitsrelevante Kommunikation zwischen Ladestation, Kund_innen und CPO erfolgt ausschließlich sicher verschlüsselt und authentifiziert. Verwendet werden dafür ausschließlich sichere Algorithmen und Protokolle (insbesondere: TLS 1.2 und TLS 1.3) mit entsprechenden Signaturen und andere Methoden um die Authentizität der Gegenstelle sicherzustellen. (siehe auch Negativliste Angreifer für Ergänzungen)
3. Die Konfiguration der Systeme und Kommunikation ist grundsätzlich einwandfrei, d.h. Ladestationen, Kommunikationsnetz-Komponenten und Systeme des CPO sind alle korrekt konfiguriert und können miteinander auf IP- bzw. Transportebene Daten austauschen.
4. Es gibt keine längerfristigen, großflächigen Störungen, die die gesamte Kommunikation unterbinden.

5. Die für die Funktion der Ladeinfrastruktur relevanten Dienste wie z.B. Domain Name System (DNS), Network Time Protocol (NTP), usw. sind korrekt konfiguriert und für alle Komponenten erreichbar.
6. Die Kommunikation zwischen CPO und Ladestation verwendet das bereits erwähnte Protokoll OCPP.

Positivliste Angreifer: Die Studie nimmt an, dass Angreifer die technischen Möglichkeiten besitzen, um:

1. **Einzelne Systeme teilweise oder vollständig zu kompromittieren** bzw. im Extremfall Vollzugriff darauf zu erlangen. Typische Beispiele sind IoT-Komponenten mit bekannten Schwachstellen, aber auch Übernahme von PCs, Routern, Modems oder Smartphones am Kommunikationspfad, z.B. über Malware-Infektionen oder Phishing-Angriffe. Eine besondere Betrachtung ist für die vollständige Kompromittierung von Ladestation und/oder des CPMS/CPO notwendig, siehe folgende Negativliste.
2. **Sich lesend auf allen Protokollebenen in die Datenkommunikation zwischen zwei Systemen einschalten können**, sowohl im Internet als auch im LAN bzw. Heimnetz der Kund_innen. Im kommunikationstechnischen Sinn ist das ein typischer (nur-lesender) Man-in-the-Middle (MitM) Angriff.
3. **Sich auf allen Protokollebenen möglicherweise lesend und schreibend in die Datenkommunikation zwischen zwei Systemen einschalten können** – als klassischer schreibender MitM. Daten in IP-Paketen können beliebig umgeschrieben werden, ohne dass die Gegenstelle das auf IP- oder Transportebene bemerken könnte (nur durch zusätzliche softwaremäßige Absicherung/Verschlüsselung/Signatur auf höheren Ebenen, z.B. TLS – siehe Voraussetzungen im vorigen Absatz).
4. Die Annahme (3) schließt ein, dass evtl. für die Funktion der Ladeinfrastruktur **relevante Dienste wie z.B. DNS oder NTP durch den Angreifer manipuliert werden können**.

Negativliste Angreifer: Die Studie nimmt an, dass Angreifer folgende Möglichkeiten NICHT haben:

1. **Aufbrechen von (TLS 1.2 und 1.3) Verschlüsselung sowie von verwendeten Signaturen**. Genauer: ein MitM kann, ohne im Besitz des Schlüssels (private Key oder shared secret Key) des Empfängers zu sein, die Daten einer beobachteten TLS-Verbindung weder
    a. Mitlesen,
    b. Modifizieren, noch
    c. Einen neuen Schlüssel vereinbaren
2. **Vollständige Kompromittierung der relevanten Komponenten des CPOs**. Andernfalls (d.h. bei Möglichkeit der vollständigen Übernahme der Komponenten des CPO, bzw. bei Entschlüsselung von dessen verschlüsselter Kommunikation) sind weitere Sicherheitsbetrachtungen gegenstandslos, da die notwendigen Steuersignale für den Angriff für externe Beobachter nicht von legitimen Steuersignalen des CPOs unterscheidbar sind.
3. **Die Kommunikation zwischen CPO und einem Großteil der Ladestationen komplett zu unterbinden** (also den Datenaustausch zu verunmöglichen).
4. **Keine zusätzlichen Kommunikationskanäle außer den explizit erwähnten haben**. In einigen Fällen nimmt die Studie explizit an, dass z.B. eine Ladestation sowohl im Heimnetz (LAN) der Kund_innen hängt, als auch über eine eigene Mobilfunk-Anbindung für den CPO erreichbar ist. Wichtig ist die Annahme, dass keine **weiteren, geheimen** Kommunikations-Schnittstellen vorhanden sind.

5. **Vollständige Kompromittierung und Möglichkeit der Fernsteuerung aller Ladestationen eines CPOs**. In diesem Fall ist nach unserer Einschätzung, ähnlich wie bei der Kompromittierung des CPO, keine realistische Abwehr eines Angriffs auf das Netz möglich.

3.4.5 Kategorisierung von Angriffen (Systeme, Netze, User)

Ein gängiger Ansatz bei Sicherheitsanalysen ist die Segmentierung der Architektur und eine separate Analyse jedes einzelnen Segments. Danach bezieht sich die CIA-Triade (siehe Definition in Kapitel 1.1 (14)) auf drei Hauptkonzepte, die in der Cybersicherheit gelten: **Vertraulichkeit, Integrität und Verfügbarkeit**. Vertraulichkeit (**C**onfidentiality) bedeutet, dass die ausgetauschten Daten nur für autorisierte Endpunkte zugänglich sein sollten; zum Beispiel sollte ein Austausch zwischen Ladestation und CPO für Dritte nicht zugänglich sein. Integrität (**I**ntegrity) bedeutet, dass die über eine Verbindung ausgetauschten Informationen nicht von einem unbefugten Dritten, z. B. einem Man-in-the-Middle, verändert werden. Verfügbarkeit (**A**vailability) bezieht sich auf die Fähigkeit, jederzeit auf Daten (Quelle) zugreifen zu können, ohne dass dies spürbare Auswirkungen auf die kommunizierenden Anwendungen hat.

Außerdem können sich Cyber-Bedrohungen auf mehreren Ebenen auswirken, vor allem auf der sozialen, der cyber- und der physischen Ebene. Auf der **sozialen Ebene** (S) zielen die Angriffe darauf ab, das menschliche Verhalten zu manipulieren, indem sie das Vertrauen ausnutzen, das zwischen den Menschen und den verwendeten Hilfsmitteln, wie z. B. Elektrofahrzeugen, besteht. Darüber hinaus zielen einige Angriffe darauf ab, private Informationen über das Verhalten der Kund_innen und Informationen über die Fahrzeugmarke, die Anzahl der Fahrzeuge usw. preiszugeben. Auf der **Cyber-Ebene** (C) zielen die Angriffe in erster Linie darauf ab, die Privatsphäre der Kund_innen zu verletzen, einschließlich der Erfassung von persönlichen Identifikationsmerkmalen, privaten Schlüsseln, Bankinformationen und allen anderen Daten, zu denen Kund_innen Zugang gewähren oder die mit dem Laden eines Elektrofahrzeugs in Verbindung stehen. Angriffe auf der **physischen Ebene** (P) beinhalten die Möglichkeit, Geräte zu zerstören, Schaden anzurichten (ähnlich wie bei der bereits in Kapitel 2.2 erwähnten Kaspersky-Schwachstelle) und so weiter.

Wir fassen einige mögliche Angriffe in verschiedenen Kategorien mit ihren Merkmalen und Beschreibungen in Tabelle 2 zusammen, indem wir die drei Sicherheitsaspekte aus der CIA-Triade und die Auswirkungsebenen kombinieren.

Tabelle 1: Mögliche Angriffe, Angriffsziele und Gefährdungen der unterschiedlichen Sicherheitskategorien der Ladeinfrastruktur. | CPO=Charge Point Operator | CSO=Charge Station Owner (Kund_in) | CPMS=Charge Point Management System | CP=Charge Point (Ladestation) | EV=Electrical Vehicle (E-Fahrzeug) | IoT=Internet of Things (SmartHome Geräte) |

Angriffe	Angriffsziel	Confidentialitv	Integritv	Availabilitv	Social	Cvber-phvsical	Physical	Beispiel
DoS	CPO, CSO, CPMS, CP			X	X	X	X	CPO ist nicht länger erreichbar und/o die Kommunikation mit Ladestationen zwecks Konfiguration, Steuerung und Updates ist nicht mehr möglich.

Bruteforce	CP/EV/IoT	X			X	X	X	Bruteforcing von Passwörtern im Heimnetz und Erlangung von Zugriff auf IoT-Geräte inkl. der Ladestation.
Delay	CPO, CSO, CPMS, CP			X		X	X	Verursachung von Kommunikationsverzögerungen oder vollständiges Unterdrücken der Ladestations-Kommunikation zwecks Steuerung, Updates, Zeitsynchronisation, etc.
Eavesdropping	CPO, CSO, CPMS, CP	X			X	X		Aufzeichnen sensibler Information am Übertragungsweg zwischen Ladestation und CPMS oder einem Endgerät der Kund_innen. Beinhaltetet z.B. auch unverschlüsselte Kommunikation mit dem Web-Interface der Ladestation.
Impersonating	CPO, CSO		X			X		Kommunikation mit dem CPMS unter Verwendung gefälschter Ladestations- oder Kund_innen-Identität (bzw. CPMS/CPO-Identität).
MitM	CPO, CSO	X	X			X	X	Manipulation von Konfigurations-, Update-, oder Steuerungsnachrichten (im Wertebereich, d.h. Ändern von Datenfeldern, oder im Zeitbereich, d.h. Verzögerung von Nachrichten).
Misinformation	CPO, CSO		X		X		X	Gezielte, missbräuchliche Veränderung des Ladeverhalten von Kund_innen. Z.B. Laden in einer bestimmten geographischen Region aufgrund falscher Tarifinformation fördern, während ohnehin Überlastsituation im Netz herrscht.
Charging profile manipulation	CPO, CSO		X	X	X	X	X	Durch Manipulation des Ladeprofils Fehlfunktionen des Elektrofahrzeugs oder in der elektrischen Infrastruktur am Installationsort verursachen.
…								

Betrachtet man darüber hinaus die Architektur praktischer Systeme, die derzeit in Österreich verwendet werden, so muss eine große Anzahl von Verbindungen analysiert und gesichert werden. Abbildung 2 zeigt u.a. potentielle Ziele – und Quellen – für Angriffe.

3.5 Generische Sicherheitsanalyse auf Protokollebene

OCPP ist ein Protokoll, das eine standardisierte Kommunikation zwischen Ladestationen und dem zentralen System des CPO (CPMS) ermöglicht, und zwar ohne Kosten oder Lizenzierung. OCPP hat sich in Europa zum de-facto-Standard für die Kommunikation zwischen Backend (CPMS) und Ladestationen für Elektrofahrzeuge entwickelt. Aufgrund der bereits weiten Verbreitung von OCPP ist der Erfolg und Zeitrahmen potentieller Nachfolger (insbesondere IEC 63110, siehe Kapitel 2.1) derzeit nicht absehbar. Unter Zuhilfenahme weiterer Protokolle wie z.B. vom Open Inter-Charge Protocol (OICP) unterstützt OCPP auch einen Roaming-Betrieb für Ladeinfrastruktur, analog zum Mobilfunk: Kund_innen können Ladestationen anderer Ladestationsbetreiber nützen, sofern diese Betreiber Roaming-Vereinbarungen mit dem Betreiber der Kund_innen haben (genauer: mit dem Betreiber von deren Ladekarte) und die Ladestation für Roaming-Anwendungen freigeschaltet wurde. OCPP benötigt für den Betrieb eine aufrechte Konnektivität auf IP-Ebene aller beteiligten Geräte, womit sich die Angriffsfläche dieser Geräte möglicherweise vergrößert. Die neueste Version, OCPP 2.0.1, verbessert die Sicherheitsmaßnahmen, wie z. B. den sicheren Verbindungsaufbau, Sicherheitsereignisse/ Protokollierung und sichere Firmware-Updates. Die Open Charge Alliance hat eine Empfehlung für die Ergänzung von OCPP 1.6-J mit Sicherheitskomponenten (OCPP 1.6-J Security WhitePaper, [41]) nachgereicht, da Sicherheitsaspekte zuvor vollständig an die einzelnen OCPP-Implementierer delegiert wurde. Wesentliche Erweiterungen betreffen sicheren Verbindungsaufbau, sicheres Log, und sicheres Firmware-Update.

Ungesicherter Transport mit Basisauthentifizierung, TLS mit Basisauthentifizierung und TLS mit client-seitigen Zertifikaten sind die drei von OCPP 2.0.1 unterstützten (und über das Security WhitePaper für OCPP 1.6-J nachträglich rückportierten) Sicherheitsprofile, die in Tabelle 2 aufgeführt sind. Wie viele Sicherheitsrahmenwerke für Kommunikationsnetze verfolgt OCPP damit drei spezifische Ziele:

- **Vertraulichkeit der Kommunikation**: Verschlüsselung wird eingesetzt, um die Vertraulichkeit der Kommunikation zwischen Einheiten zu schützen und zu verhindern, dass Unbefugte die Kommunikation abfangen oder verändern können.
- **Authentifizierung des CPO**: Es ist wichtig, dass die Ladestation überprüfen kann, ob sie mit dem richtigen CPMS kommuniziert, da dies sonst zu einer Kommunikation mit potentiellen Angreifern (MitM) führen könnte.
- **Authentifizierung der Ladestation**: Der CPMS muss in der Lage sein, Ladestationen zu authentifizieren, um Angreifer daran zu hindern, gefälschte Ladestationen zu erstellen, die sich als legitime Ladestationen ausgeben und anmelden.

Eine weitere, nachdrücklich empfohlene Sicherheitsmaßnahme ist das mit den OCPP-Erweiterungen mögliche, CPMS-gesteuerte, TLS-gesicherte Firmware-Update der Ladestationen. Von der vorher als Standard verwendeten Aktualisierung mittels FTP wird aufgrund von schwerwiegenden Sicherheitsbedenken abgeraten: FTP überträgt ausschließlich Klartext, einschließlich der Authentifizierungsdaten (Username, Passwort). Einem MitM-Angreifer stehen folglich bei FTP-Aktualisierung der Ladestations-Firmware alle Wege der Kompromittierung offen, sofern nicht zusätzliche Sicherungsmaßnahmen getroffen werden (siehe detaillierte Diskussion in Kapitel 5.4.1.7).

3.5.1 OCPP-basierte Steuerung von Ladestationen

Die Ansteuerung der Ladeinfrastruktur mit dem Ziel der Netzstabilisierung und/oder Flexibilisierung des Energiehandels wird technisch durch die OCPP-Nachricht SetChargingProfile (genauer: das Nachrichtenpaar SetChargingProfile.req/-.conf in OCPP 1.6 bzw. SetChargingProfileRequest/-Response in OCPP 2.0.1) umgesetzt. Mit dieser Nachricht kann ein CPMS das Lastprofil von Ladestationen konfigurieren, und somit die Maximalleistung von Ladepunkten begrenzen. Da die vorliegende Studie eine standardkonforme Lösung erarbeiten soll, wird im weiteren Verlauf (ausschließlich) die Sicherheit dieser Steuerungsmöglichkeit von Ladestationen der Kund_innen durch CPOs analysiert.

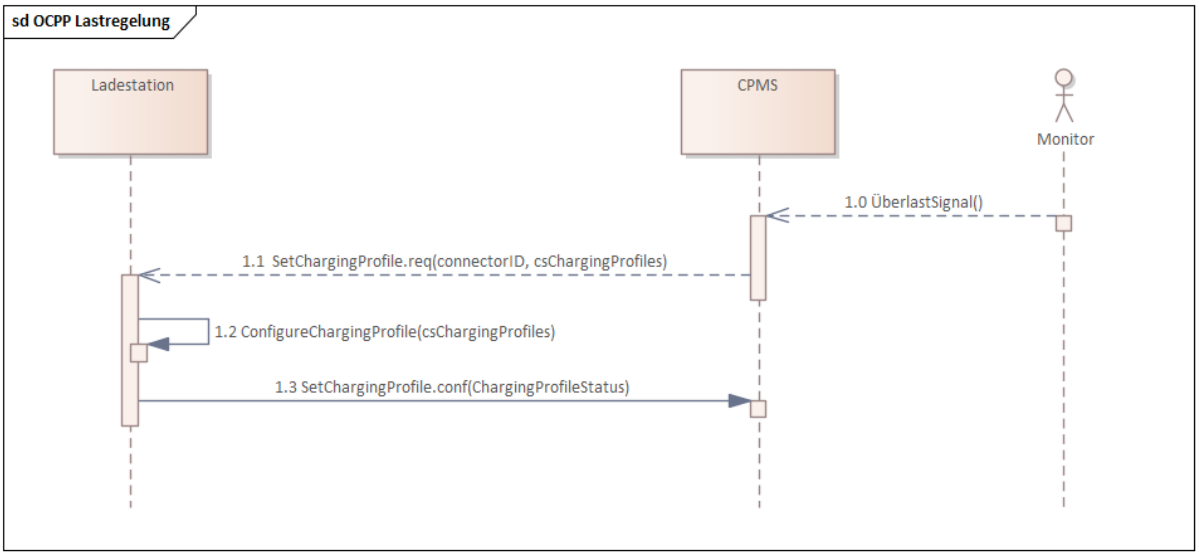

Abbildung 8: OCPP-basierte Steuerung der Ladestation der Kund_innen durch das CPMS des CPO.

Abbildung 8 stellt in einem Sequenzdiagramm dar, wie ein CPO (bzw. dessen CPMS) nach Vorgabe des OCPP-Protokolls die Leistung der Ladestation von Kund_innen steuern kann.

0. (Nicht OCPP-Standard): Der CPO (CPMS in Abbildung 8) erhält über nicht näher definierte Quellen oder Sensoren die Information, dass in einem Teilnetz Überlast herrscht (oder Notwendigkeit für Flexibilisierung besteht) und die Last reduziert werden muss. Als ersten

Schritt muss der CPO jene Ladestationen ausfindig machen, die er in diesem Teilnetz steuern kann. Die Logik der Auswahl geeigneter Ladestationen und entsprechender Leistungsregelungen ist komplex, aber Lösungen sind nicht Teil dieser Sicherheitsstudie.

1. In der Folge muss der CPO an alle betroffenen Ladestationen (im Sequenzdiagramm wird der Einfachheit halber nur eine Ladestation dargestellt) mittels der OCPP-Nachricht SetChargingProfile.Request ein geeignetes Lastprofil übermitteln. Dieses Lastprofil besteht aus einem oder mehreren Lastprofilen und deren Start bzw. Dauer (Datenfeld: csChargingProfiles). Der Aufbau des Ladeprofils wird im Anschluss an diese Liste detaillierter besprochen.
2. (Nicht OCPP-Standard): Nach Empfangen des vom CPMS gesendeten SetChargingProfile.Request verarbeitet die Ladestation die angeforderten Lastprofile csChargingProfiles (im Sequenzdiagramm durch eine proprietäre, nicht OCPP-spezifizierte Nachricht ConfigureChargingProfiles angedeutet). Die Steuerung kann Ladeprofile für einzelne Ladepunkte der Ladestation oder ein Gesamt-Ladeprofil für die Ladestation vorgeben. Letzterer Fall bedeutet, dass die Ladestation die Lastreduktion eigenständig auf die aktiven Ladepunkte verteilen muss.
3. Die Ladestation meldet dem CPMS mit der OCPP-Nachricht SetChargingProfile.Confirm den Empfang und die Verarbeitung der CPO-Aufforderung zur Leistungssteuerung. Über den Rückgabewert (ChargingProfileStatus) im SetChargingProfile.Confirm teilt die Ladestation dem CPMS mit, ob eine Änderung des Lastprofils gemäß der Vorgabe beabsichtigt wird oder nicht.

Wichtige, weitere Anmerkungen zum Sequenzdiagramm in Abbildung 8:

1. Voraussetzung für den Versand der OCPP-Nachrichten zwischen CPMS und Ladestation ist das Vorhandensein (oder vorherige Erstellen) einer geeigneten, gesicherten Verbindung auf Transportebene (TCP & TLS). Falls diese Verbindung noch aufgebaut werden muss, ist mit zusätzlicher Verzögerung zu rechnen (Detailanalyse dazu folgt in den Kapiteln 4 und 5).
2. Der CPO bzw. CPMS hat beim Erhalt des ChargingProfileStatus (zulässige Werte: *Accepted*, *Rejected*, oder *NotSupported*) in der OCPP SetChargingProfile.Confirm Nachricht keine bindende Information darüber, ob und wann genau die Ladestation die angeforderte Leistungsregelung durchgeführt hat. Während die negative Rückmeldung der Ladestation (Werte: Rejected oder NotSupported) den Misserfolg der Anfrage eindeutig ausdrückt, stellt Accepted eine Absichtserklärung der Ladestation dar. Eine Ende-zu-Ende Rückmeldung der Ladestation an den CPMS könnte erst zu einem späteren Zeitpunkt erfolgen – denkbar wäre z.B. über eine OCPP MeterValues Nachricht, wie in Kapitel 5.1 und 5.2 beschrieben.
3. Nicht Teil der Studie, aber relevant und aus rechtlicher Sicht zu bewerten ist, ob und inwieweit ein derart engmaschiges – für die technische Realisierung vermutlich aber unverzichtbares – Monitoring der Ladeleistung der Ladestation der Kund_innen mittels OCPP MeterValue Meldungen einen unzulässigen Eingriff in die Privatsphäre der Kund_innen gemäß DSGVO darstellt.

```
“csChargingProfiles”: {
    “chargingProfileId”: 1379023,
    “chargingProfileKind”: “Absolute”,
    “chargingProfilePurpose”: “TxProfile”,
    “chargingSchedule”: {
        “chargingRateUnit”: “W”,
        “chargingSchedulePeriod”: [
            {
               “limit”: 22000.0,
               “startPeriod”: 0
            },
            {
               “limit”: 11000.0,
               “startPeriod”: 900
            },
            {
               “limit”: 5500.0,
               “startPeriod”: 1800
            },

            {
               “limit”: 22000.0,
               “startPeriod”: 3600
            }],
         “duration”: 3600
     },
     “stackLevel”: 0,
     “transactionId”: 5387813,
     “validFrom”: “2023-01-22T12:00:00+00:00”,
     “validTo”: “2023-01-23T11:59:59+00:00”
}
```

Abbildung 9: Beispiel für OCPP Ladeprofil mit Leistungsbegrenzung 22kW ab Zeitpunkt 0 (12:00), 11kW ab 15 Minuten, 5.5kW ab 30 Minuten, 22kW ab 60 Minuten. Erstellt/modifiziert/korrigiert auf der Basis von [42]

Ein Beispiel für ein hypothetisches OCPP-Ladeprofil ist in Abbildung 9 ersichtlich. Ausgehend von der aktuell konfigurierten Maximalleistung der Ladestation fordert der CPO mit diesem Lastprofil von der Ladestation eine zeitgesteuerte Reduktion der Ladeleistung an. Die Ladestation soll dabei die angeforderte Maximalleistung folgendermaßen anpassen:

1. Max. 22kW Ladeleistung ab dem Zeitpunkt 0, entsprechend 12.1.2023, 12:00, bzw. ab dem Erhalt und der Bearbeitung des Lastprofils
2. 11kW nach 15 Minuten (zum Zeitpunkt 22.1.2023, 12:15)
3. 5.5kW nach 30 Minuten (zum Zeitpunkt 22.1.2023, 12:30)
4. 22 kW ab dem Zeitpunkt 22.1.2023, 13:00)

Der letzte Wert soll für die angesagte Dauer gelten – oder bis zum Erhalt neuer Lastprofile.

Wesentliche Anforderung an die Sicherheit der Ladestationssteuerung ist demzufolge das Sicherstellen, dass das durch den CPO versandte Ladeprofil der Ladestation (a) zeitgerecht und (b) korrekt und unverändert zugestellt und (c) von dieser bearbeitet wird.

Herausforderung für den CPO ist dabei in einem zeitkritischen Anlassfall rechtzeitig:

1. Die möglichen bzw. am besten geeigneten zu regelnden Ladestationen auszuwählen.
2. Die Regelungsanforderungen (SetChargingProfile) an diese Ladestationen möglichst zeitnah zu versenden
3. Auf eventuelle Ablehnungen bzw. Fehlermeldungen in Echtzeit zu reagieren um die notwendige Gesamtreduktion der Leistung zu erreichen (z.B.: Ladestation lehnt Reduktion ab: wähle stattdessen andere Station aus und fordere deren Leistungsreduktion an).
4. Eine gesicherte Ende-zu-Ende Rückmeldung zu erlangen, ob die angeforderten Leistungsregelungen tatsächlich zeitgerecht und in vollem Umfang durchgeführt wurden.

Ein erfolgreicher Angriff lässt sich aus OCPP-Sicht auf folgende Fälle reduzieren: es gelingt dem Angreifer

1. **Selber falsche Lastprofile an Ladestationen auszusenden, und/oder**
2. **Bestimmte Werte in vom CPO gesendeten Lastprofilen vor dem Empfang durch die Ladestation zu modifizieren und/oder**
3. **Zu verhindern, dass die Ladestation die Lastprofile des CPO überhaupt oder zeitgerecht empfängt, und/oder**
4. **Falsche Statusmeldungen der Ladestationen an den CPO zu senden oder die Werte legitimer Statusmeldungen vor dem Empfang durch den CPO zu verändern.**
5. **Zu verhindern, dass Statusmeldungen von der Ladestation an den CPO zugestellt werden.**

Je mehr dieser Aspekte ein Angreifer beeinflussen kann, je (zeit)genauer und synchronisierter seine eigene Steuerung und Manipulation erfolgt, und je mehr Ladestationen er kompromittieren kann, desto höher die Wahrscheinlichkeit und größer seine Möglichkeiten, dass er mit genau koordinierten Aktionen das gesamte Energienetz gefährden kann – bis hin zum totalen Kollaps (Blackout).

In der Folge werden die möglichen, generischen, vom OCPP-Protokoll vorgesehenen Sicherheitsmaßnahmen vorgestellt und analysiert.

3.5.2 Das Transport Layer Security (TLS) Protokoll

Grundlegend für die folgende Diskussion der OCPP-Sicherheit ist das von OCPP verwendete Sicherheitsprotokoll Transport Layer Security (TLS) um Verbindungen auf Transportebene abzusichern und die Kommunikationspartner zu authentifizieren. Vorbedingung ist das Vorhandensein einer TCP-Verbindung, wie später beschrieben.

Zwei Versionen von TLS sind für die Absicherung des OCPP-Protokolls zulässig, TLS 1.2 [43] sowie TLS 1.3 [44]. Die TLS-Versionen 1.0 und 1.1 wurden von der IETF 2021 offiziell als nicht mehr zulässig (deprecated) erklärt [45]. Demzufolge sind die im OCPP WhitePaper [46] genannten Ausnahmen, dass TLS 1.0 und 1.1 aus Gründen der Rückwärtskompatibilität verwendet werden können, nicht mehr zulässig: ausschließlich der Einsatz von TLS 1.2 oder TLS 1.3 gewährleistet die sichere Steuerung der Ladestationen. Für die Studie relevant sind folgende Metriken in Bezug zu TLS:

1. Wie viele Daten müssen übertragen werden, bis die Verbindung abgesichert ist? Im Detail:
    a. Wie viele Runden (Round-Trips) sind für die Absicherung notwendig
    b. Welche Datenmenge muss übertragen werden
2. Ist die Authentizität der beiden Kommunikationspartner abgesichert? D.h. hat sich keiner, einer oder beide der Kommunikationspartner kryptographisch belegbar identifizieren können oder nicht?

In der Folge wird der Verbindungsaufbau für TLS 1.2 und TLS 1.3 in Bezug auf diese Metriken betrachtet um die relevanten Details zu identifizieren. Ausgangsbasis sind die Diagramme in den Standards, die zwecks Lesbarkeit für diese Publikation angepasst wurden. Farblich hinterlegt wurden Einträge in den folgenden Diagrammen mit folgenden Farben:

1. **Blau:** die beteiligten Kommunikationspartner (Server und Client)
2. **Gelb:** gesendete Nachrichten(gruppen)
3. **Orange:** Zertifikatsaustausch zwecks kryptographischer Identifikation der Teilnehmer.
4. **Grün:** Erste Möglichkeit Nutzerdaten auszutauschen.

Aufgrund der Festlegung von OCPP auf TCP bzw. TLS/TCP wird in dieser Studie ausschließlich die Verwendung von TLS über TCP betrachtet. Diese Variante (TLS über TCP) ist Voraussetzung für eine Absicherung aller besprochenen in der Folge besprochenen Varianten und Anwendungsfälle, d.h. aller Transport-Mappings für OCPP (XML/SOAP und JSON/Websockets, siehe Kapitel 3.5.4, 3.5.5, bzw. 3.5.6).

3.5.2.1 TLS 1.2 (TCP) Verbindungsaufbau

Das Diagramm in der folgenden Abbildung 10 stellt den Aufbau einer auf Transportebene gesicherten, verschlüsselten TLS 1.2 Verbindung, einschließlich der notwendigen Nachrichten und der ausgetauschten Daten gemäß RFC 5246 [43] dar (unter der Annahme, dass Client und Server eine bestehende Verbindung auf Transportebene haben, d.h. eine TCP-Verbindung bereits aufgebaut wurde). Unter der Annahme, dass der Client auch die TCP-Verbindung aufbaut, kann die ClientHello TLS-Nachricht mit dem TCP SynAck Segment des Clients mitgesendet werden. Somit sind mindestens 3 Runden (Round-Trips) zwischen Client und Server notwendig, bis eine gesicherte TLS 1.2-Verbindung zwischen Client und Server aufgebaut ist und Anwendungsdaten übertragen werden können.

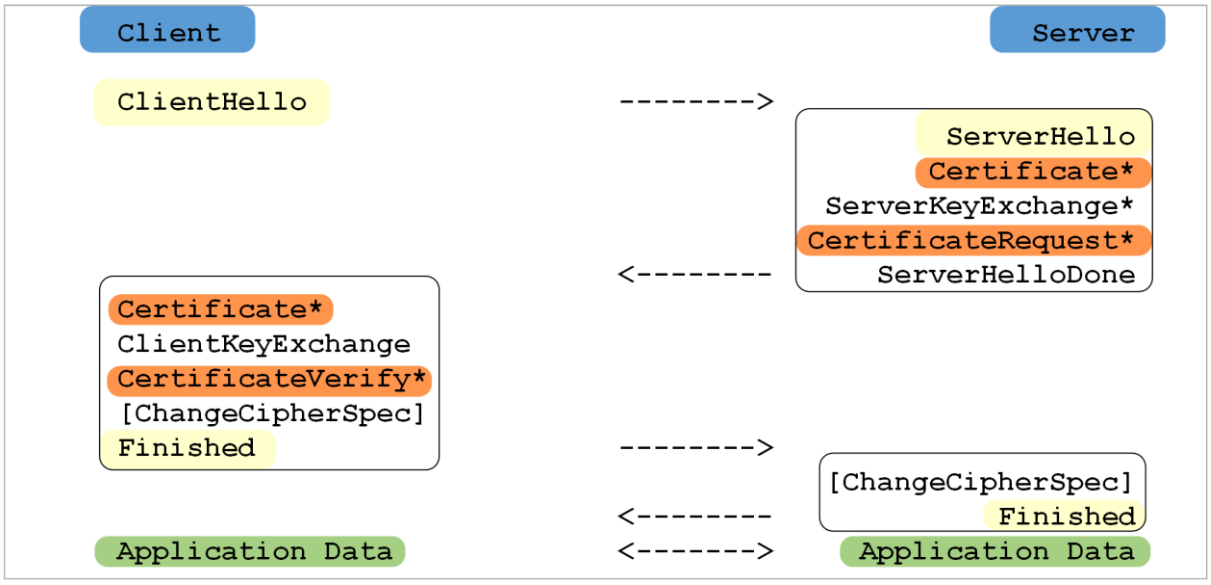

Abbildung 10: TLS 1.2 Verbindungsaufbau gemäß Fig.1 von RFC 5246 [20], ergänzt mit farblichen Hervorhebungen um die notwendigen Metriken, Nachrichten und Daten zu identifizieren.

Diese Anwendungsdaten beinhalten beispielsweise (gesicherte, mit TLS verschlüsselte) HTTP-Anfragen wie beispielsweise den WebSocket-Verbindungsaufbau (wird bei OCPP-J in der Folge besprochen).

Identifizieren muss sich der Server (rechts) beim Client mittels eines Server-Zertifikats, das der Server gemeinsam mit der ServerHello Nachricht (im gleichen TCP Segment) an den Client senden kann. Der Client kann anhand des Zertifikats und der in ClientHello und ServerHello ausgetauschten kryptographischen Daten die Authentizität des Servers überprüfen.

Gleichzeitig kann der Server auch den Client auffordern, sich zu authentifizieren (mittels CertificateRequest als Teil der ServerHello-Nachricht). Der Client wird in der Folge sein Client-Zertifikat mitschicken um seine Identität nachzuweisen. Im Kontext der vorliegenden Fernsteuerung von Ladestationen bei Kund_innen gibt es bei der Ausstellung der Zertifikate für Ladestationen größere Herausforderungen, die in den Kapiteln zu OCPP-Sicherheit (Kapitel 3.5.4, 3.5.5, bzw. 3.5.6) näher ausgeführt werden.

3.5.2.2 TLS 1.3 Verbindungsaufbau

Im Laufe der Jahre hat es Forderungen gegeben, unter anderem die Anzahl der mindestens 2 Runden (3 mit TCP-Aufbau) für das Erstellen einer TLS-Verbindung zu reduzieren. Ergebnis dieser Bestrebungen war die Definition von TLS 1.3 im Jahre 2018 (RFC 8446, [44]) durch die IETF als standardisierende Organisation. Im Vergleich zu TLS 1.2 wurde bei TLS 1.3 erreicht, dass im Falle des Aufbaus einer neuen TLS-Absicherung (ohne vorherigen Kontext) schon nach einer Runde (zwei einschließlich TCP-Aufbau) Anwendungsdaten übertragen werden können. Das Diagramm des „normalen“ TLS 1.3 Verbindungsaufbaus ist in Abbildung 11 dargestellt und zeigt, dass im TCP-Segment, in dem das ServerHello übertragen wird, bereits Anwendungsdaten enthalten sind.

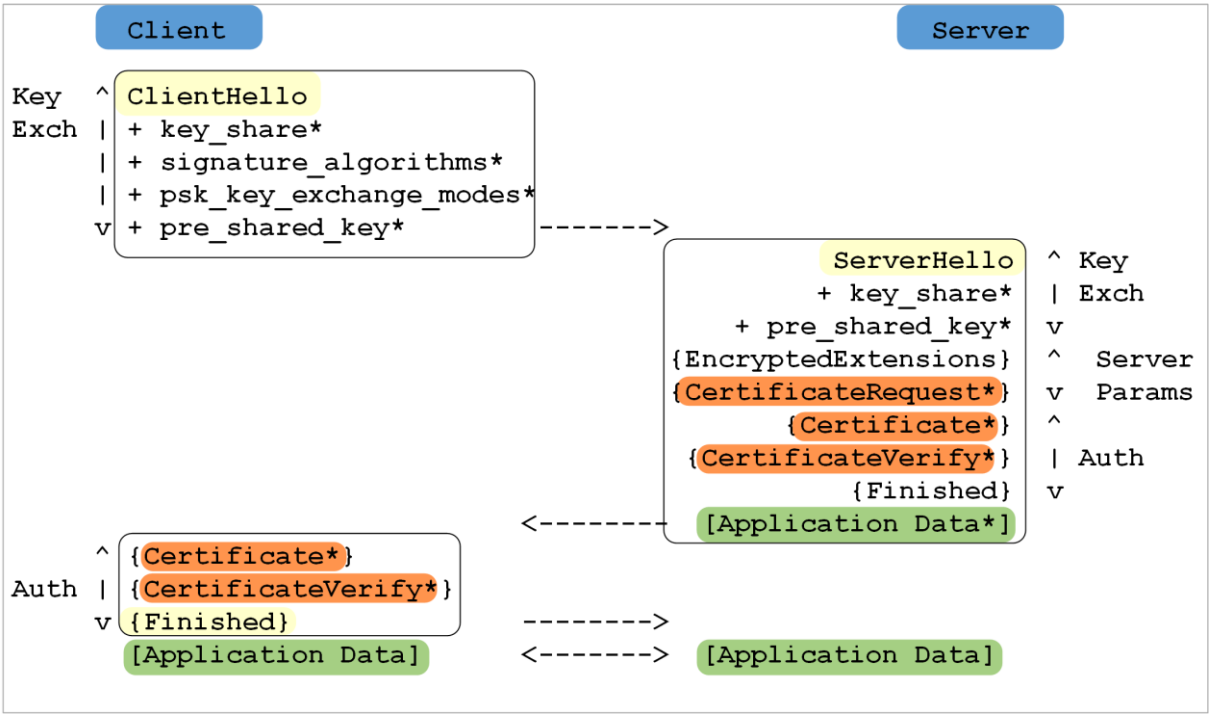

Abbildung 11: TLS 1.3 Verbindungsaufbau gemäß Fig.1 aus RFC8446 [44], ergänzt mit farblichen Hervorhebungen um die notwendigen Metriken, Nachrichten und Daten zu identifizieren

Wesentliche Neuerung in TLS 1.3 ist jedoch die Möglichkeit, den Schlüsselaustausch einer vorher bestehenden TLS 1.3 Verbindung weiter zu verwenden. Sofern ein Verbindungsaufbau gemäß Abbildung 11 bereits stattgefunden hat, kann – im Idealfall, im RFC als 0-RTT bezeichnet – das bereits ausgehandelte Schlüsselmaterial weiterverwendet werden. Client und Server können somit im Idealfall direkt, unter Verwendung des bisherigen Schlüsselmaterials Nachrichten mitschicken (siehe grün hinterlegte Datenfelder als Teil der ersten ausgetauschten Nachrichten in Abbildung 12, ClientHello und ServerHello).

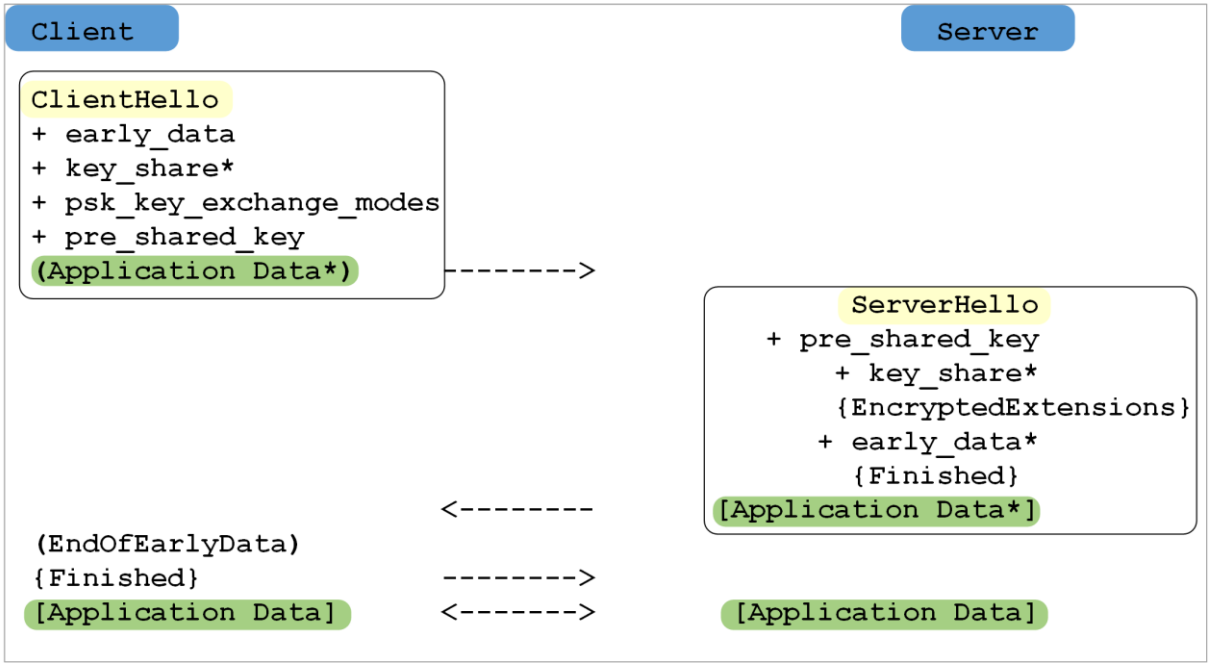

Abbildung 12: Verkürzter (0-Runden PSK, 0-RTT) TLS 1.3 Verbindungsaufbau gemäß Fig.4 von RFC8446 [21], ergänzt mit farblichen Hervorhebungen um die notwendigen Metriken, Nachrichten und Daten zu identifizieren.

Sofern die Vorbedingungen für das Weiterverwenden des Schlüsselmaterials erfüllt sind, kann 0-RTT die Reaktionszeit bzw. Zeit für den Verbindungsaufbau signifikant reduzieren.

Äußerst wichtig ist aber, bei 0-RTT eine Einschränkung in der Sicherheit zu beachten: Angreifer können bei der Verwendung von 0-RTT sogenannte Replay-Angriffe erfolgreich durchführen.

Ein Beispiel dafür: der Client führt mit TLS 1.3 und 0-RTT eine Zahlung eines Betrags X beim Server durch. Der Angreifer schneidet als MitM die Daten am Kommunikationsnetz mit. Wenn der Angreifer die aufgezeichneten Daten nochmals sendet, muss der Server auf Anwendungsebene (in unserem Fall: z.B. OCPP Protokoll oder Anwenderdaten) erkennen, dass diese Daten bereits einmal empfangen bzw. verarbeitet wurden. Andernfalls werden die wiedergesendeten Daten nochmals bearbeitet und das Konto des Clients mit 2*X belastet.

3.5.3 OCPP-Sicherheitsprofile

Für den Inhalt dieser Studie sind drei Versionen bzw. Varianten des OCPP-Standards relevant:

1. **OCPP 1.6 mit SOAP/XML** Binding (in der Folge als **OCPP-S 1.6** abgekürzt)
2. **OCPP 1.6 mit JSON/WebSocket** Binding (in der Folge als **OCPP-J 1.6** abgekürzt)
3. **OCPP 2.0.1** – unterstützt ausschließlich JSON/WebSocket.

Die Sicherheitsvorgaben und -möglichkeiten dieser drei Versionen unterscheiden sich grundlegend voneinander, weshalb eine getrennte Analyse der Sicherheit der drei Versionen notwendig ist. Die SOAP/XML-Implementierung ist historisch bedingt, da Grundlage der OCPP-Standard-Versionen 1.2 und 1.5. In OCPP 1.6 wurde neben der SOAP/XML-Variante auch JSON/WebSocket standardisiert, vor allem wegen der deutlich kompakteren Repräsentation von JSON verglichen mit XML und effizienterer Kommunikation von WebSockets gegenüber SOAP. Ein wesentlicher Grund war auch, dass OCPP-Sicherheit mit WebSockets deutlich weniger aufwändig zu implementieren ist als mit SOAP.

Aus diesem Grund trennt der OCPP 1.6-Standard [4] die entsprechenden Dokumente auf in ein generisches, transport-unabhängiges Dokument, in dem die Funktion und Nachrichten standardisiert werden (ocpp-1.6 edition 2.pdf) sowie zwei separate Dokumente, in denen die Transport-Mappings

spezifisch für SOAP/XML (ocpp-s-1.6-specification.pdf) sowie JSON/WebSockets (ocpp-j-1.6-specification.pdf) definiert werden.

3.5.4 OCPP 1.6 SOAP/XML Sicherheit

Historisch gesehen gibt der Standard für OCPP-S 1.6 keine verpflichtenden, expliziten Sicherheitsmechanismen vor. Kapitel 6.2.4 von ocpp-j-1.6-specification.pdf erwähnt, dass historisch gesehen OCPP-S Sicherheit auf Netzwerkebene verwendet hat. D.h. entweder vertrauenswürdige Netze oder VPNs zwischen Ladestation und CPO.

Kapitel 6.2 von ocpp-s-1.6-specification.pdf [4] empfiehlt zwei Sicherungsmaßnahmen:

1. SOAP-Nachrichten zwecks Wahrung vertraulichen Inhalts mit SSL/TLS zu verschlüsseln
2. Sender sollen Client-seitige Zertifikate verwenden, damit Empfänger die Authentizität des Senders sicherstellen können.

Gleichzeitig gibt das OCPP-J 1.6 Dokument in Kapitel 6.2.4 relevante Argumente, weshalb TLS-Absicherung für OCPP-S in der Praxis sehr schwierig umzusetzen ist:

1. In OCPP-S wird für jeden Nachrichtenaustausch eine eigene Verbindung aufgebaut. Sofern eine Absicherung mit TLS notwendig ist, muss diese auch jedes Mal neu verhandelt werden. Das führt zu einem hohen Rechenaufwand und hohen Verzögerungen (3 Round-trips für TCP- plus TLS 1.2 Aufbau).
2. Da bei OCPP-S auch Ladestationen als HTTP-Server aktiv sein können bzw. müssen (im Gegensatz zu OCPP-J, wo immer der Client die Websocket-Verbindung aufbaut), benötigt jede Ladestation ein Server-Zertifikat. Diese Vorgangsweise ist mit äußerst hohem Aufwand und auch Kosten verbunden. Weiters stellt sich die Frage, wie Server-Zertifikate mit Host/Domain-Namen und privaten Adressen gehandhabt werden – CPOs müssten sich vermutlich eine eigene Zertifizierungsstelle aufbauen.

Die beiden verbleibenden, vom Standard genannten Optionen sind ebenfalls nicht akzeptabel bzw. implementierbar:

3. Von einer Verwendung „vertrauenswürdiger Netze“ und dem Vertrauen auf Verschlüsselung durch die Kommunikationsnetze muss aufgrund von Kompromittierungen anderer Technologien, die diese Mechanismen verwendet haben, jedenfalls abgeraten werden. Details dazu werden in der Besprechung von OCPP-J 1.6 im folgenden Unterkapitel ausgeführt.
4. Die Implementierung dedizierter VPNs zwischen Ladestation und CPO ist aufgrund von diversen Gründen schwer realisier- bzw. vorstellbar, wie beispielsweise Bootstrapping („wie baue ich eine vertrauenswürdige, erste Verbindung auf?“), Overhead (Daten, Rechenleistung für Verschlüsselung), Update (wie wird der VPN aktualisiert), oder Architektur (eigene Verbindung notwendig für jeden Nachrichten-Austausch).

Die genannten Gründe zusammenfassend muss davon ausgegangen werden, dass OCPP-S 1.6 (die SOAP-Variante der OCPP 1.6-Implementierung) für einen sicheren, steuernden Zugriff auf Ladestationen einen sehr hohen Aufwand benötigt und deutlich ineffizienter ist als die OCPP-J 1.6 Variante. In der Analyse in Kapitel 5 wird im Detail auf die Herausforderungen und Nachteile eingegangen, um OCPP-S Implementierungen standardkonform abzusichern.

3.5.5 OCPP 1.6 JSON/WebSocket Sicherheit

Mit der Standard-Version 1.6 hat OCPP zusätzlich zu dem bis dahin ausschließlich verwendeten SOAP/XML Mapping auch die Unterstützung für JSON/WebSocket vorgesehen. Wesentliche Vorteile

sollen eine kompaktere Darstellung bzw. Repräsentation von Daten sein sowie eine deutlich verbesserte, effizientere Kommunikation bei der Kommunikation mit Webservern. Große Vorteile bringt das WebSocket-Protokoll, wenn sich der Client mit einer privaten IP-Adresse hinter einem NAT befindet, d.h. für den Server ansonsten nicht oder nur mit komplexen technischen Maßnahmen (Port-Forwarding am NAT-Router) erreichbar wäre. Das Mapping von OCPP auf die Transport-Option JSON/Websocket (d.h. OCPP-J 1.6) ist in der Datei ocpp-s-1.6-specification.pdf beschrieben.

Für WebSockets gibt es, wie beim HTTP-Protokoll, zwei Varianten: gesicherte und ungesicherte Kommunikation. Da die unsichere Variante, analog zum HTTP-Protokoll, die Daten unverschlüsselt überträgt, bietet sie keinen Schutz gegen Angreifer. Aus diesem Grund wird in der Folge dieser Studie ausschließlich die mit TLS gesicherte Variante von WebSockets behandelt.

Bei der sicheren Kommunikation mittels WebSockets baut der Client in einem ersten Schritt eine sichere TCP und TLS-Verbindung zum Server auf. In dieser gesicherten Verbindung wird das WebSocket-Protokoll (über einen HTTP-Aufruf, der eine zusätzliche Runde benötigt) gestartet. Die verhandelte WebSocket-Verbindung kann anschließend für bidirektionale Kommunikation zwischen Client und Server verwendet werden. Wesentlicher Vorteil des WebSocket-Protokolls ist eine sichere Kommunikation über NAT-Grenzen hinweg: Da viele Web-Clients auf Rechnern in lokalen Netzen der Kund_innen laufen, erlaubt diese Form der Kommunikation den Aufbau einer semi-persistenten Verbindung von einem Client in einem typischerweise privaten Adressbereich zu einem Server mit einer öffentlichen IP-Adresse. Der Server kann anschließend (bei Bedarf) mittels der aufgebauten, bestehenden, sicheren, bidirektionalen Verbindung Daten an den Client senden.

Das Dokument ocpp-j-1.6-specification.pdf analysiert bzw. spezifiziert in Kapitel 6 die Sicherheit für zwei Varianten:

1. Sicherheit auf Kommunikationsnetzebene (Kapitel 6.1 von OCPP-J 1.6 [4])
2. OCPP-J über TLS (Kapitel 6.2 von [4])

Diese beiden Varianten werden in der Folge im Detail analysiert.

3.5.5.1 Sicherheit auf Kommunikationsnetzebene

In Kapitel 6.1 von OCPP-J 1.6 [4] wird explizit die Möglichkeit der Absicherung auf Kommunikationsnetzebene besprochen. Mögliche Interpretationen bzw. Implementierungen wären etwa „vertrauenswerte Kommunikationsnetze“, die auf physischer Schicht durch Verschlüsselung abgesichert werden (insbesondere Mobilfunknetze) oder VPN-Mechanismen.

Vor einer (ausschließlichen) Absicherung gemäß OCPP-J 1.6 Kapitel 6.1 (d.h.: ohne zusätzliche Ende-zu-Ende TLS Absicherung) muss aus folgenden Gründen bzw. mit folgenden Beispielen explizit und dringend gewarnt werden:

1. Bezüglich „vertrauenswerte Kommunikationsnetze“ ein Beispiel aus dem Bereich Mobilfunk: die Verschlüsselung von 3G und 4G Kommunikationsnetzen gilt derzeit als sicher. Die Verschlüsselung von 2G-Mobilfunknetzen ist nach heutigem Stand einfach kompromittierbar – sie kann mit geringem Aufwand in Echtzeit entschlüsselt werden. Beim BMW-Connected-Drive-Hack [47] wurde bereits 2015 erfolgreich und pressewirksam vorgeführt, wie man alle über dieses System verfügenden ca. 2,2 Millionen Fahrzeuge komplett kontrollieren kann: Türen und Fenster öffnen und schließen, Motor starten, Hupe aktivieren, usw. Mit einem sogenannten „Downgrade“-Angriff mit einem IMSI-Catcher wird die sichere 3G- oder 4G-Mobilfunk-Technologie auf 2G gezwungen – um anschließend die Verschlüsselung aufzubrechen und die im Klartext vorliegende Kommunikation nach Belieben zu verändern. Die Notwendigkeit der Rückwärts-Kompatibilität von Technologien und Protokollen ist

historisch verankert – und es gilt als gesichert, dass ähnliche Angriffe auch in Zukunft erfolgen werden.
2. Selbst wenn Teilpfade der Kommunikation vertrauenswürdig sind (z.B. geschützte Unternehmens-Kommunikationsnetze, oder 3G/4G verschlüsselte Teilstrecken), ist nicht garantiert, dass der gesamte Kommunikationspfad zu Kund_innen sicher ist. Das Übertragen von unverschlüsselten Nachrichten auf Teilstrecken der Kommunikationsnetze birgt die Gefahr, dass Angreifer (z.B. über Botnetze oder Malware) über Zugriff auf die entsprechenden Komponenten verfügen und die übertragenen Daten beliebig modifizieren können.
3. Das Implementieren geeigneter VPN-Technologien zwecks Ende-zu-Ende-Absicherung der Kommunikation zwischen Ladestation und CPO kann eine Lösung sein. Im Kontext von NAT und Kund_innen-Infrastruktur stellt sich jedoch das Problem geeigneter Lösungen, Wartung und Updates. Man kann davon ausgehen, dass, abgesehen von der proprietären Lösung, eine VPN-Lösung mit gleichen Sicherheitsmerkmalen wie TLS deutlich fordernder und komplexer zu realisieren ist als die von OCPP-J alternativ vorgesehene Absicherung mittels TLS.

Aus den genannten Gründen wird von der OCPP-Absicherung auf Kommunikationsnetz-Ebene gemäß Kapitel 6.1 OCPP-J 1.6 abgeraten und in der Folge die Sicherheit der standardisierten TLS-Lösung (Kapitel 6.2) analysiert.

3.5.5.2 OCPP-J über TLS

Die Absicherung von OCPP-J 1.6 über TLS wird im Dokument ocpp-j-1.6-specification.pdf [4] in Kapitel 6.2 definiert. Folgende Einschränkungen und Empfehlungen trifft der Standard:

1. OCPP-J 1.6 verwendet TLS 1.2 [43] mit RSA Schlüsselgröße <=2048 bytes (Kapitel 6.2.1). Begründen lässt sich eine Höchst-Schlüssellänge mit möglichen Hardware-Limitierungen von Ladestationen. Die Studienautoren erachten 2048 bytes aus Sicherheitsgründen jedoch als Mindestanforderung.
2. Ein von einer autorisierten Zertifizierungsstelle signiertes Server-Zertifikat wird für das CPMS empfohlen (ist aber nicht verpflichtend)
3. Die Authentifizierung der Ladestation erfolgt mittels HTTP Basic Authentication (über eine TLS-verschlüsselte Verbindung). Gemäß Kapitel 6.2.2 ist als Username der Identifier der Ladestation zu verwenden und als Passwort ein 20 byte langer String, der auf der Ladestation gespeichert wird. Optionen für die Speicherung des Passworts auf der Ladestation werden besprochen, u.a. bei der Herstellung oder Installation der Ladestation (mit sicherer Übertragung des Passworts an den CPO als Betreiber des CPMS). Das Passwort sollte eindeutig pro Station sein – falls nicht möglich, erwähnt der Standard eine Möglichkeit der Konfiguration mit Master-Key und folgendem Setzen mittels OCPP ChangeConfiguration.req().
4. Empfohlen wird im Standard [4] weiters:
    a. Das Konfigurieren des Passworts beim ersten Booten der Ladestation (BootNotification der Ladestation erzwingt ChangeConfiguration.req des CPMS mit neuem Passwort, erst nach Bestätigung über ChangeConfiguration.conf der Ladestation bestätigt das CPMS die BootNotification).
    b. Eine aktive Anomalieerkennung und Überwachung durch den CPO um z.B. das Registrieren sehr vieler neuer Ladestationen (evtl. als Folge eines geleakten Master-Passwords) zu erkennen und Gegenmaßnahmen zu treffen.
    c. Verlässliches, sicheres und persistentes Speichern des Passworts auf der Ladestation, da diese bei Verlust des Passworts nicht mehr zum CPMS verbinden kann und Vor-Ort Service notwendig ist.

    d. Sicheres Speichern des Passworts auf der Ladestation (Hash, Salt) um zu verhindern, dass bei Auslesen des Passwortspeichers der Angreifer die Daten missbräuchlich verwenden kann.
5. Während eine Übernahme einer Ladestation, die noch nicht konfiguriert wurde (d.h. noch den Master-Key verwendet, der möglicherweise an den Angreifer geleaked wurde) durch den Angreifer möglich ist, erwähnt Kapitel 6.2.2 explizit **Angriffe, die mittels der Passwort-Mechanismen unterbunden werden sollen bzw. können**:
    a. Reservieren einer Ladestation, indem Nachrichten gefälscht werden, die die Ladestation als besetzt markieren (Angriff auf Verfügbarkeit).
    b. Ladesession einer öffentlichen Ladestation über gefälschte Nachrichten als gestoppt kennzeichnen um weniger zu zahlen (Energiediebstahl bei öffentlichen Ladestationen, wirtschaftlicher Verlust).
    c. Senden gefälschter Transaktionen oder Fehlermeldungen von konfigurierten Ladestationen (Angriff auf Verfügbarkeit, Überlast CPMS oder finanzieller Nachteil für Eigentümer der verwendeten TokenIDs).
6. Kapitel 6.2.3 erwähnt den beabsichtigten Schutz der Sicherheitsmaßnahmen von OCPP-J 1.6:
    a. Verschlüsselung der Verbindung zwischen Ladestation und CPMS
    b. Ladestations-Authentifizierung beim CPMS (mittels HTTP Basic Authentication über TLS-gesicherte Verbindungen)
    c. Authentifizierung des CPMS gegenüber der Ladestation (mittels TLS-Zertifikat).
7. Kapitel 6.2.3 erwähnt mögliche Schwachstellen, für die OCPP-J 1.6 keine Lösung bietet
    a. Änderung der zu übertragenden Messwerte auf dem Pfad zwischen Messgerät und CPMS durch einen Angreifer (Messgerät müsste als Gegenmaßnahme jeden Messwert signieren)
    b. Authentifizierung der Kund_innen
    c. Physische Angriffe auf die Ladestation

Zusammenfassend gliedert sich eine gemäß OCPP-J 1.6 angebundene Ladestation deutlich besser in die geplante Architektur der Ladeinfrastruktur ein und bietet mehr Flexibilität, geringere Menge an Datenübertragung und bessere Sicherheit als OCPP-S 1.6. Eine detaillierte Diskussion der Sicherheitsmerkmale und -defizite folgt in Kapitel 5 anhand der konkreten Anwendungsfälle.

3.5.6 OCPP 2.0.1 Sicherheit

OCPP 2.0.1 ist eine Weiterentwicklung von OCPP 1.6 um den Standard gemäß den Erfahrungen aus dem Praxiseinsatz zu erweitern. Neu in OCPP 2.0.1 ist die Definition von drei Sicherheitsprofile, um den unterschiedlichen Sicherheitsanforderungen gerecht zu werden. Diese Profile sind in Tabelle 2 beschrieben. Das Profil "Basissicherheit" umfasst keine Authentifizierung des CPMS oder Maßnahmen zum Aufbau eines sicheren Kommunikationskanals. Hintergrund des Profils ist der mögliche Einsatz von OCPP 2.0.1 in vertrauenswürdigen Netzen – wobei analoge Anmerkungen wie in Kapitel 3.5.5.1 für OCPP-J 1.6 gelten. **Daher muss festgehalten werden, dass das Sicherheitsprofil „Unsecured Transport“ die Anforderungen dieser Studie NICHT erfüllt.**

Tabelle 2: OCPP Profile für OCPP 2.0.1 - gemäß Tabelle 11 in Kapitel 1.3 von OCPP-2.0.1_part2_specification.pdf [48]

Profile	CP Authentication	CPMS Authentication	Communication Security
Unsecured Transport with Basic Authentication	HTTP Basic Authentication	None	None
TLS with Basic Authentication	HTTP Basic Authentication	TLS authentication using Certificates	TLS

TLS with Client-side Certificates	TLS authentication using Certificates	TLS authentication using Certificates	TLS

In Tabelle 12 des Standards [48] wird definiert, dass Ladestation (CP) und CPMS jeweils nur ein Sicherheitsprofil unterstützen können. Das Sicherheitsprofil muss konfiguriert werden, bevor die OCPP-Kommunikation möglich ist. Wenn Ladestation oder CPMS versuchen, eine Verbindung mit einem anderen Profil herzustellen, sollte die Gegenstelle die Verbindung beenden. Um den aus anderen Bereichen bekannten „Downgrade-Angriffen“ vorzubeugen, legt A00.FR.005 fest, dass eine nachträgliche Änderung des Profils nicht Teil der OCPP-Spezifikation ist und auf anderem Wege erfolgen muss - insbesondere eine Reduktion der Sicherheitsvorkehrungen.

3.5.6.1 Unsecured transport with basic authentication

Wie bereits festgehalten, wird dieses Sicherheitsprofil ohne TLS-Schutz für ungeeignet für die Steuerung von Ladestationen erachtet. Die CS-Authentifizierung erfolgt über HTTP mit Anmeldedaten, es sind keine Maßnahmen zur Sicherung des Kommunikationskanals vorgesehen.

3.5.6.2 TLS with basic authentication

Beim Profil TLS mit Basisauthentifizierung wird der Kommunikationskanal mit Transport Layer Security (TLS) gesichert. Der CPMS authentifiziert sich mit einem TLS-Serverzertifikat. Die Ladestation authentifiziert sich mit HTTP Basic Authentication.

- **Ladestations-Authentifizierung**: Die Ladestation authentifiziert sich gegenüber dem CPMS über HTTP mittels Username und Password. Da in diesem Profil TLS für die Absicherung der Transportebene des Kommunikationsnetzes verwendet wird, werden die Anmeldedaten verschlüsselt übertragen.
- **CPMS-Authentifizierung**: Der CPMS fungiert als TLS-Server. Beim Aufbau der TLS-Verbindung muss sich der Server mittels gültigem Server-Zertifikat identifizieren. Wenn der CPMS kein oder kein gültiges Zertifikat bereitstellt, bricht die Ladestation die Kommunikation ab.
- **Kommunikationskanal**: Beim Profil TLS mit Basisauthentifizierung wird der Kommunikationskanal nach dem ersten Handshake mit TLS gesichert. Nicht alle TLS-Konfigurationen und Cipher Suites bieten ausreichende Sicherheit: Der CPMS muss RSA- und ECDH-Chiffre-Suites unterstützen. Veraltete Cipher Suites sind nicht zulässig, und die Verbindung wird bei Verwendung einer solchen mit der Meldung "*Invalid TLS cipher suite*" abgebrochen. Darüber hinaus dürfen Ladestationen und CPMS nur TLS 1.2 oder eine höhere Version verwenden, andernfalls wird die Verbindung mit der Meldung "*Invalid TLS version*" abgebrochen.

3.5.6.3 TLS with client side certificates

Beim Profil TLS mit Client-Zertifikaten wird der Kommunikationskanal mit TLS gesichert. Sowohl die Ladestation als auch das CPMS authentifizieren sich mit Zertifikaten.

- **Ladestations-Authentifizierung:** Die Ladestation authentifiziert sich gegenüber dem CPMS mit Hilfe des Ladestations-Zertifikats. Bei OCPP 2.0.1 ist ausschließlich JSON/WebSocket unterstützt, so dass die Ladestation als Client und der CPMS als Server agiert. Ladestationen und CPMS überprüfen einige der Zertifikatsfelder und brechen die Verbindung ab, falls Zertifikate nicht vorhanden oder ungültig sind, bzw. Felder ungültig sind.
- **CPMS-Authentifizierung:** Ähnlich wie im vorigen Abschnitt muss sich auch das CPMS über ein gültiges Zertifikat als Server identifizieren, andernfalls wird die Verbindung abgebrochen.
- **Kommunikationskanal:** Wie im vorigen Fall wird der Kommunikationskanal mit TLS gesichert.

Das Security WhitePaper für OCPP-J 1.6 beschreibt die Anwendung der Sicherheitsmaßnahmen und Authentifizierungsmechanismen von OCPP 2.0.1 für OCPP 1.6.

4 Machbarkeitsanalyse und mögliche Reaktionszeiten

Um die Machbarkeit der Flexibilisierung bzw. Netzstabilisierung mittels privater Ladestationen zu untersuchen, und damit die Sicherheitsbetrachtungen in dieser Studie zu motivieren, werden wir im Folgenden untersuchen, ob erreichbare Latenzen gängiger Internetanbindungen (bzw. die resultierenden Reaktionszeiten des Systems) den Anforderungen dieser Vorgehensweise gerecht werden. Latenz bezeichnet dabei die Verzögerung eines IP-Pakets gegebener Größe auf einem Kommunikationspfad (z.B. bei der Übertragung zwischen CP und CPMS). Als Reaktionszeit wird in der Folge die (untere Schranke der) Zeit bezeichnet, die zwischen dem Eintreffen eines Bedarfs für Laststeuerung beim CPMS entsteht und der Bestätigung der Ladestation über eine erfolgreiche Reduktion der Ladeleistung.

4.1 Metriken für Latenzen und Reaktionszeiten

Zur Beurteilung der gemessenen Latenzzeiten muss ein genauer Blick auf die verwendeten Kommunikationsprotokolle geworfen werden, da möglicherweise mehrere IP-Pakete zwischen den Kommunikationspartnern ausgetauscht werden müssen, bis die tatsächlich notwendige Protokollnachricht zugestellt wurde. Um daher die tatsächliche Verzögerung (=Reaktionszeit) vom Bekanntwerden der Notwendigkeit einer Ladeleistungsreduktion bis zur tatsächlichen Leistungsreduktion feststellen zu können, werden möglicherweise die Latenzen mehrerer Pakete in beide Richtungen tragend.

Gemäß der Annahme wird üblicherweise das OCPP Protokoll zur Kommunikation zwischen CPO und Ladestationen eingesetzt, wobei sich einerseits OCPP-S 1.6 und, andererseits, OCPP-J 1.6 und OCPP 2.0 wesentlich in diesem Aspekt aufgrund ihrer eingesetzten Technologien und Protokolle unterscheiden. Während OCPP-S 1.6 auf das Simple Object Access Protocol (SOAP) [49] als Transportmechanismus aufbaut, um Anfragen in beide Richtungen durchzuführen, wird bei OCPP-J 1.6 bzw. OCPP 2.0.1 für den gleichen Zweck das Websocket-Protokoll [50] genutzt.

SOAP sieht keine persistente Verbindung vor, was bedeutet, dass zur Durchführung einer Anfrage, im vorliegenden Fall beispielsweise eine Ladeleistungsreduktion, zunächst eine gesicherte TLS-TCP/IP Verbindung aufgebaut werden muss. Dies erfordert nicht nur einen vollständigen zusätzlichen Roundtrip in Folge des TCP-Handshakes, im wünschenswerten Fall einer TLS-gesicherten Verbindung muss zusätzlich auch ein TLS-Handshake durchgeführt werden, bevor die Schlüssel für die gesicherte Verbindung verhandelt sind und die tatsächliche Nachricht verschlüsselt (gesichert) gesendet werden kann.

Websocket setzt zwar wie SOAP zum Zwecke der Verbindungsherstellung auf HTTP (und auf TLS) auf, führt aber dann einen Protokollwechsel durch, um nicht mehr an die Protokollsemantik von HTTP gebunden zu sein. Websocket ist es damit möglich, eine persistente Verbindung aufrecht zu erhalten, die sowohl Client als auch Server zum Senden von Nachrichten nutzen können und damit zusätzliche Verzögerungen von Protokoll-Handshakes zu vermeiden.

Neben den unterschiedlichen Protokollversionen sind außerdem zwei Zeitspannen von Relevanz:

- Unmittelbar relevant ist die Zeitspanne vom Bekanntwerden der Notwendigkeit einer Steuerung der Ladeleistung bis zur tatsächlichen Leistungsänderung. Um zur Stabilisierung von Frequenzabweichungen im europäischen Verbundnetz eingesetzt werden zu können, darf diese Reaktionsgeschwindigkeit den Bereich von wenigen Sekunden nicht überschreiten.
- Weiters ist jedoch relevant, welche Zeitspanne zusätzlich eingeplant werden muss, bis der CPO über den Erfolg einer beauftragten Ladeleistungsänderung informiert wird. Da private Ladestationen in einem nicht überwachten Umfeld installiert werden, kann der CPO nicht mit Sicherheit davon ausgehen, dass eine Ladeleistungsänderungsanfrage den gewünschten Effekt hat.

4.2 Messaufbau

Die Messungen wurden in Kooperation mit einem CPO bzw. Backend-Betreiber (illwerke vkw) gemäß dem in Abbildung 13 dargestellten Aufbau durchgeführt. Die Ladestation wurde durch einen Server mit Mobilfunk-USB-Modem, ausgestattet mit einer SIM-Karte mit privatem APN des Backend-Betreibers, implementiert. Die Datenpakete für die Messungen wurden über das CPMS des Backend-Betreibers an einen Mess-Server im Kommunikationsnetz der TU Wien weitergeleitet. Als Betriebssystem für den Messrechner wurde Linux verwendet – aufgrund des deutlich deterministischeren Verhaltens, der besseren Konfigurierbarkeit und der Möglichkeiten genauer Zeitmessung verglichen mit Windows oder anderen Betriebssystemen.

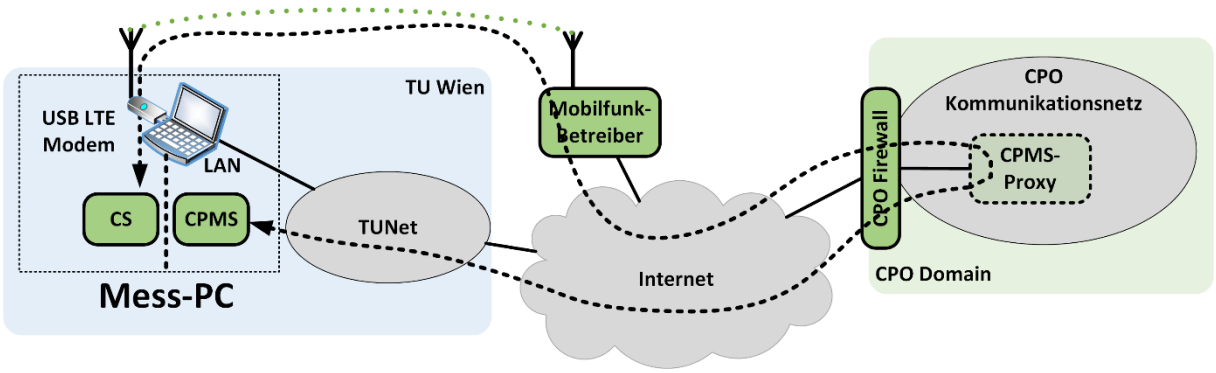

Abbildung 13: Messaufbau für Messung der Einweg-Verzögerungen von IP Paketen in Abhängigkeit ihrer Größe für verschiedene Mobilfunk-Technologien (jeweils Uplink und Downlink, 2G, 3G, 4G).

Für die Messungen wurden UDP-Datenpakete verwendet um den Einfluss und die Unsicherheiten von TCP-spezifischen Algorithmen (Flusskontrolle, NAGLE Algorithmus, usw.) zu vermeiden. Neben den Latenzen des primär relevanten Teilpfads zwischen Mobilfunkmodem und CPO (obere, strichlierte Linie in Abbildung 13 zwischen CS bzw. USB LTE Modem links und CPMS Proxy rechts) beinhaltet der Übertragungsweg den zweiten Teilpfad über das öffentliche Internet vom Backend-Betreiber zum Server der TU Wien (untere, strichlierte Linie zwischen CPMS-Proxy rechts und CPMS bzw. LAN links). Die zusätzliche Latenzzeit des zweiten Teilpfads liegt im Bereich weniger Millisekunden. Dieser Messaufbau wurde ausgewählt, um die TU-eigenen Server verwenden zu können und die Messung vom Backend-Betreiber und dessen Systemen weitgehend unabhängig zu gestalten. Die Abweichung der Latenzen aufgrund des zusätzlich gemessenen Teilpfads Backend - TU Wien ist von der Größenordnung her für die relevante Steuerungsfunktionalität vernachlässigbar.

Mobilfunknetze sind von der Charakteristik her sehr stark asymmetrisch: die Übertragung des gleichen Datenpakets im Uplink (vom Mobiltelefon zum Internet) dauert signifikant länger als die Übertragung des gleichen Datenpakets im Downlink (vom Internet zum Mobiltelefon). Aufgrund dieser Eigenschaft wurde die Messung von Einweg-Latenzen (One-way delay) statt der gängigen Round-trip Verzögerungen als unverzichtbar erachtet. Das bedeutet, dass statt dem für Messungen der Latenz gängigen ping-Tool (basierend auf ICMP Echo Request) komplexere Tools verwendet werden und

zusätzliche Randbedingungen erfüllt werden mussten. Als wesentliche Voraussetzung müssen für das Messen von Einweg-Verzögerungen die Uhren von Sender und Empfänger hochgenau synchronisiert sein.

Umgehen lässt sich die Voraussetzung synchroner Uhren indem Sender und Empfänger auf dem gleichen Server implementiert werden. Der Server verfügt in diesem Fall über zwei Netzwerkschnittstellen für die Mobilfunkverbindung und die gewöhnliche kabelbasierte Internetanbindung.

Ein praktisches Hindernis in einem derartigen Setup ist, dass die Protokollstacks gängiger Betriebssysteme Netzwerkpakete gar nicht erst in das Internet senden, wenn sie feststellen, dass sie selbst (d.h. eine andere Schnittstelle am gleichen System) der Paketempfänger sind. Gelöst wurde diese Problematik beim Messaufbau mittels zweier unterschiedlicher Linux Network Namespaces für die jeweiligen Netzwerkschnittstellen, um die Empfängerseite komplett von der Senderseite zu trennen. Hierbei verfügen die verschiedenen Namespaces über jeweils eigene, vollständig getrennte Netzwerkstacks, was beispielsweise die IP-Konfiguration und die Routingtabellen umfasst. Es ist damit sichergestellt, dass die gesendeten Pakete tatsächlich über die untersuchte Strecke gesendet werden, und, da Empfänger und Sender auf die gleiche Hardwareuhr zurückgreifen, dass eine exakte Uhrensynchronisation gegeben ist.

Zur Durchführung der Messungen wurde das Representative Delay Measurement Tool (RDM) [51] verwendet, das im Gegensatz zu einem simplen ping in der Lage ist, Einwegverzögerungen zu messen, indem der Empfangszeitpunkt in Antwortpaketen mitübermittelt wird. RDM arbeitet mit vordefinierten Szenarien, die eine vordefinierte Abfolge von zu übermittelnden Paketen festlegen um auf diese Weise die Wiederholbarkeit identer Messungen zu ermöglichen.

Eine große Herausforderung bei Mobilfunkmessungen ist, dass bestehende Datenverbindungen bei längerer Nichtverwendung im Hintergrund abgebaut (bzw. auf eine Minimalkapazität herabgesetzt) werden. Sinn dieser Maßnahme ist die Optimierung der Gesamtkapazität des Mobilfunknetzes, bzw. Nutzung der vorhandenen Mobilfunkressourcen für andere Kund_innen. Die Definition der Dauer von „Nichtverwendung“ ist Technologie- und Mobilfunknetz-spezifisch, meistens ein paar Sekunden. Sobald wieder Daten übertragen werden, baut das Mobilfunknetz den Träger im Hintergrund wieder auf und weist der Verbindung Ressourcen zu. Das erste nach der Sendepause übertragene Datenpaket hat jedoch aufgrund der Vorgangsweise eine deutlich höhere Latenz als bei vorhandener Verbindung.

Für die Messungen wurde daher als relevant erachtet:

1. Aufgrund der asymmetrischen Mobilfunknetze die **korrekte Richtung der Datenübertragung** zu verwenden (die Anforderung des CPMS zur Leistungssteuerung an die Ladestation verwendet den Downlink, die Antwort der Ladestation an das CPMS den Uplink des Mobilfunknetzes)
2. Aufgrund der asymmetrischen Mobilfunk-Kapazitäten **Einweg-Messungen mit unterschiedlichen Paketgrößen zu verwenden** (da die Paketgröße als entscheidender Faktor die Höhe der Latenz mit beeinflusst).
3. **Mehrere Varianten und Intervalle von Inaktivitäten (Sendepausen) am Mobilfunkpfad zu messen**. Die zwischen CPMS und Ladestation über das Mobilfunknetz ausgetauschten Daten sind auch ein möglicher Kostenfaktor für den CPO (Mobilfunkdaten, Multiplizitätsfaktor durch Anzahl der Ladestationen).

4.3 Messergebnisse

Um einen Überblick über die zu erwartenden Latenzen zu erstellen, ermitteln wir die Latenzzeiten für übertragene Pakete für verschiedene Datenpaketgrößen zwischen 50 Bytes und 1500 Bytes und für verschiedene Mobilfunktechnologien (2G/3G/4G). Als Anhaltspunkt hat das csChargingProfile in Abbildung 9 beispielsweise eine Größe von 806 Bytes – reale Ladeprofile können sowohl kleiner als auch größer sein. Da die Verfügbarkeit moderner Mobilfunkgenerationen vom Installationsstandort abhängt, ist eine Anbindung über den vergleichsweise alten 2G-Standard – vor allem im ländlichen Raum – realistisch und muss betrachtet werden.

Das gemessene Szenario sieht eine Leistungsreduktion im Auftrag des CPO vor. Hierfür muss die Kommunikation zum relevanten Zeitpunkt serverseitig initiiert werden, d.h., das erste Paket nach einer möglicherweise längeren Leerlaufperiode wird über den Downlink des Mobilfunkmodems gesendet. Wir nutzen daher den gleichen Nachrichtenablauf in unseren Experimenten.

Wie oben erläutert, besteht die Möglichkeit, dass das erste Paket nach einer längeren Leerlaufperiode einer höheren Latenzzeit unterliegt. Um dies zu berücksichtigen, führen wir Messungen mit kurzen Intervallen zwischen einzelnen Datenpaketen von 500msec, aber auch mit langen Intervallen von 30s aus.

Die untenstehenden Abb. 14-16 zeigen die Auswertung der Messergebnisse:

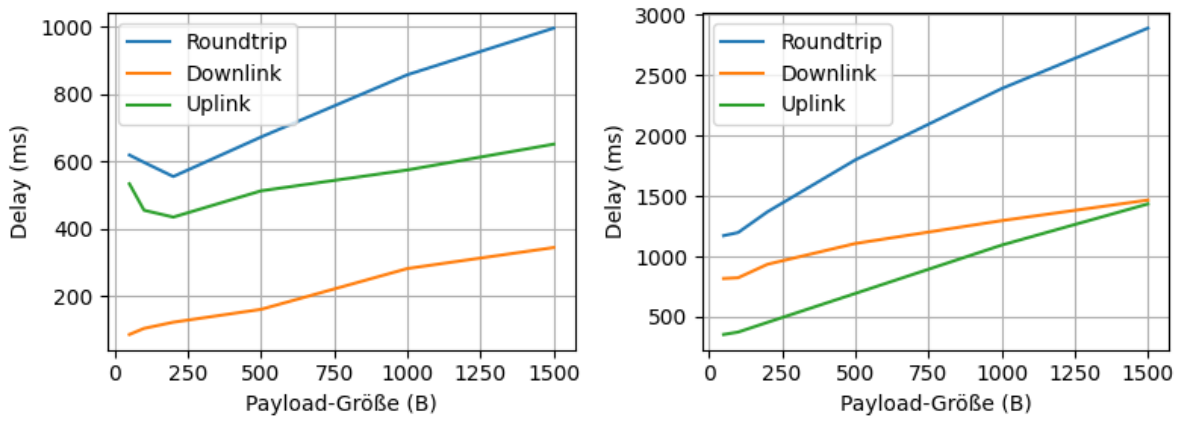

*Abbildung 14: Gemessene Paketlaufzeiten bei **2G**-Anbindung und Probe-Intervallen von 500ms (links) und 30s (rechts).*

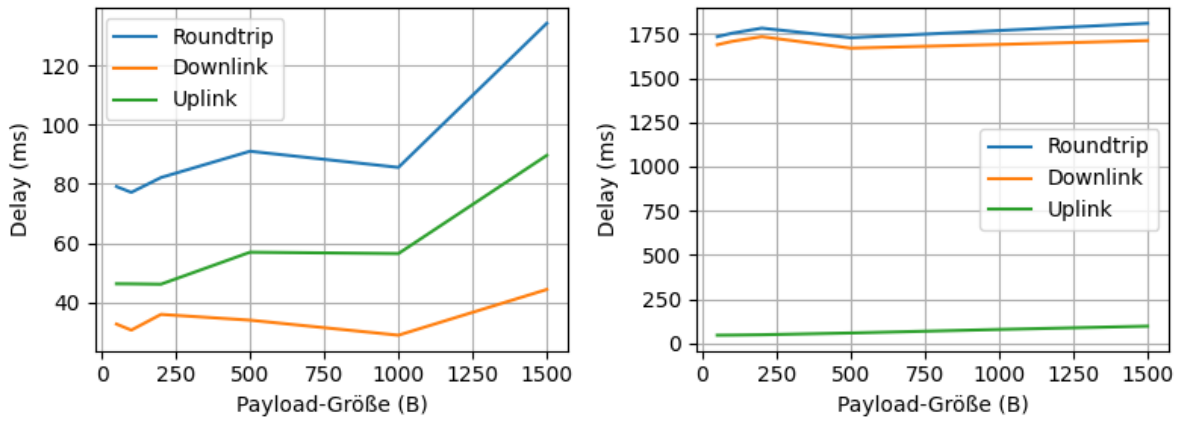

*Abbildung 15: Gemessene Paketlaufzeiten bei **3G**-Anbindung und Probe-Intervallen von 500ms (links) und 30s (rechts).*

.

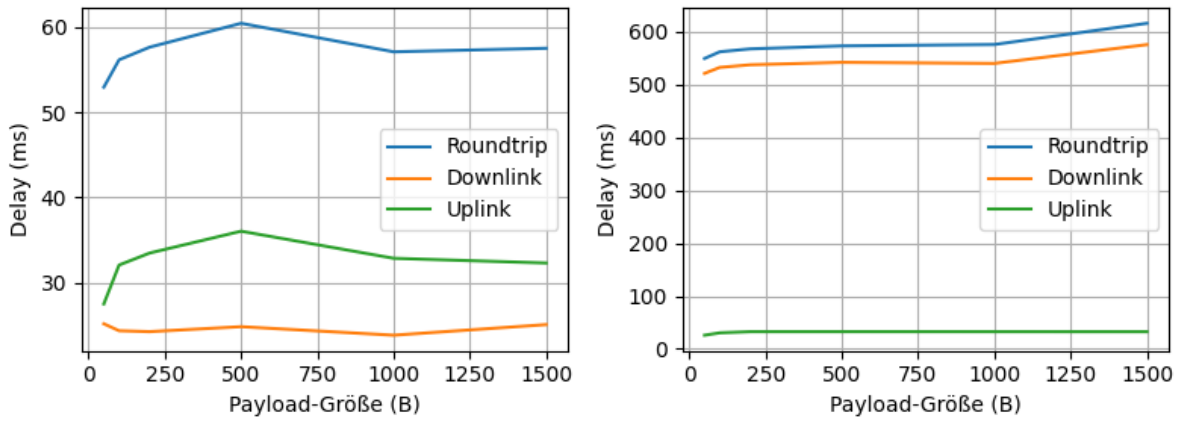

*Abbildung 16: Gemessene Paketlaufzeiten bei **4G**-Anbindung und Probe-Intervallen von 500ms (links) und 30s (rechts).*

Die Diagramme in Abbildung 14 bis Abbildung 16 zeigen die Verzögerung von Datenpaketen als Funktion der Paketgröße (in Bytes) für unterschiedliche Mobilfunktechnologien: 2G (Abbildung 14), 3G (Abbildung 15) und 4G (Abbildung 16). Getrennt aufgetragen werden die Verzögerungen für Uplink, Downlink und Roundtrip (Uplink + Downlink + Bearbeitungszeit Server).

Die Diagramme auf der linken Seite zeigen die Verzögerung bei einem kontinuierlichen Fluss von Messpaketen (alle 500ms), während die Diagramme der rechten Seite die Verzögerung bei sporadisch gesendeten Paketen (alle 30s) angeben.

Deutlich sichtbar auf den Diagrammen der linken Seite ist das asymmetrische Verhalten der Mobilfunkpfade im Normalbetrieb: die Verzögerung im Downlink ist aufgrund dessen höherer Kapazität deutlich geringer als die Verzögerung im Uplink. Auf den Diagrammen der rechten Seite sieht man eine deutliche Auswirkung der langen Sendepause: das Mobilfunknetz reduziert während der 30 Sekunden die Kapazität des Mobilfunkpfads auf ein Minimum (ggf. nur Signalisierungskanäle offen). Die erste Nachricht (entsprechend der Anforderung des CPMS zur Reduktion der Ladeleistung der Ladestation) wird im Downlink (orange) gesendet und hat (aufgrund des notwendigen Wiederaufbaus des Mobilfunkträgers) eine um Größenordnungen höhere Verzögerung verglichen mit dem Normalbetrieb: 800-1500ms für 2G, ca. 1700ms für 3G und ca. 550ms für 4G – bei Verwendung desselben Modems.

Die Messergebnisse entsprechen in mehreren Punkten den Erwartungen:

- Eine tendenzielle Erhöhung der Latenzzeit ist durch die durch die endliche Übertragungsbandbreite gegebene Serialisierungsdauer des übertragenen Pakets („transmission delay“) erwartet.
- Wie oben erläutert, ist bei dem ersten nach einer längeren Leerlaufperiode übertragenen Paket eine höhere Latenz möglich (und realistisch). Dieser Effekt kann in Plots mit langem Probe-Intervall beobachtet werden.
- Im Gegensatz hierzu ist in Plots mit niedrigem Probe-Intervall zu beobachten, dass Pakete im Downlink eine nennenswert niedrigere Latenz haben als im Uplink. Dieser Beobachtung entspricht üblichen Asymmetrien, wie sie bei Internetanbindungen im Consumer-Bereich anzutreffen sind.

Unbedingt erwähnenswert ist, dass bei 3G die Downlink-Latenz nach einer Pause in absoluten Werten deutlich HÖHER ist als die Werte von 2G Netzen. Die plausible Erklärung ist, dass 2G wahrscheinlich weniger agressiv optimiert und weniger Aufwand für den Wiederaufbau des Mobilfunkträgers nach der Pause benötigt. Der 3G Uplink wird jedoch anscheinend gleichzeitig mit dem 3G Downlink wieder

alloziert: demzufolge fallen für die folgende Bestätigung der Ladestation an den CPMS im Uplink die normalen Latenzen an, die auch bei kontinuierlichen Datenströmen sichtbar sind (sichtbar im Vergleich Abbildung 15 links vs rechts, grüne Linie – Achtung wegen unterschiedlicher Y-Werteskalen).

Das kritischste Szenario für den untersuchten Einsatzzweck ist eine über 2G angebundene Ladestation nach einer längeren Inaktivitätszeit der Mobilfunkverbindung. Um dieses Szenario näher zu beleuchten, und Worst-Case-Abschätzungen zuzulassen, stellen wir unsere beobachteten Verteilungen von Einwegverzögerung und Paketumlaufzeit in nachfolgenden Abbildung 17 dar.

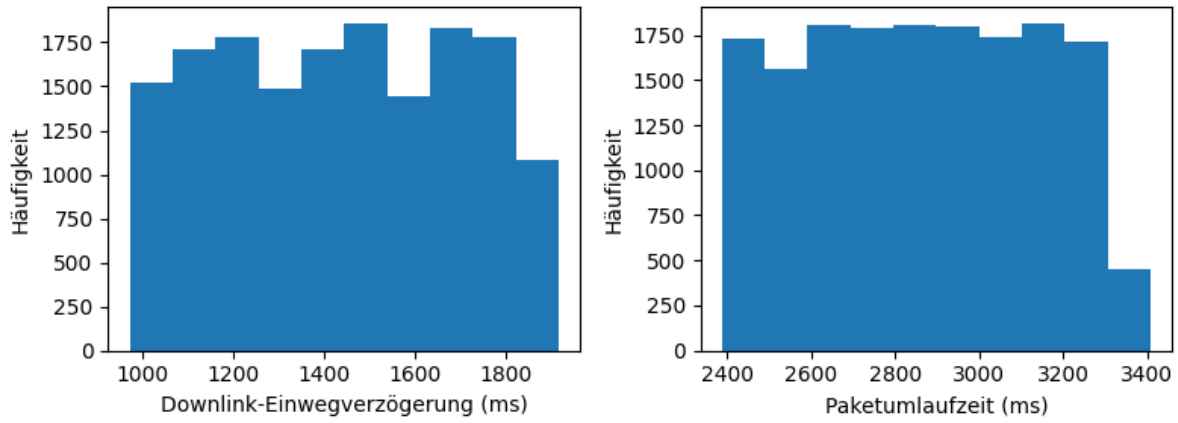

*Abbildung 17: Gemessene Paketlaufzeiten bei **2G**-Anbindung, Probe-Intervallen von 30s und einer Payload-Größe von 1500B.*

Daraus ergibt sich eine Paketumlaufzeit – also Verzögerung vom Absetzen des Befehls zur Reduktion der Ladeleistung der Ladestation durch den CPMS bis zum Eintreffen der Bestätigung, jedoch OHNE die Bearbeitungszeit der Ladestation – von bis zu 3,4 Sekunden.

4.4 Evaluierung der Reaktionszeiten für repräsentative Anwendungsfälle

Um die oben festgestellten Latenzzeiten auf die hier untersuchten Anwendungsfälle umzulegen, muss ein detaillierterer Blick auf die für die Ladeinfrastruktur genutzte Netzwerkkommunikation geworfen werden. Wie oben bereits umfassend dargelegt, wird für die Ladeleistungsreduktion die SetChargingProfile-Nachricht des OCPP-Protokolls genutzt. Ein SetChargingProfile-Request wird damit im Bedarfsfall vom CPMS zur Ladestation gesendet, um die Ladeleistung zu reduzieren.

4.4.1 Reaktionszeit bei Verwendung von WebSocket

Wird OCPP über WebSocket genutzt, ist, wie oben beschrieben, eine persistente Websocket-Verbindung zwischen Ladestation und CPMS bereits vorhanden, über die der SetChargingProfile-Request gesendet wird, womit keine Roundtrips vor dem Senden der Nachricht nötig sind. Gemäß der OCPP-Spezifikation ist der Payload einer SetChargingProfile-WebSocket-Nachricht aufgebaut, wie beispielhaft in Abbildung 18 gezeigt.

```
[ 2,
  "09ea13b4-e087-4167-b4ea-a0735af79ec2",
  "SetChargingProfile",
  {
    "connectorId": 1,
    "csChargingProfiles": { … }
  }
]
```

Abbildung 18: Beispiel einer SetChargingProfile-Nachricht, wie sie in der WebSocket-Payload übertragen wird. Die bereits oben erläuterte csChargingProfiles-Struktur wurde hier zwecks Übersichtlichkeit ausgelassen.

Die csChargingProfiles-Struktur, welche bereits in Abbildung 9 dargestellt wurde, wurde in Abbildung 18 zwecks Übersichtlichkeit ausgelassen. Zwecks effizienter Übertragung werden im produktiven Einsatz üblicherweise semantisch nicht erforderliche Leerzeichen und Zeilenumbrüche innerhalb der JSON-Daten entfernt. In dieser kompakten Darstellung nimmt die SetChargingProfile-Nachricht in Abbildung 18 und Abbildung 9 549B ein. Zur Übertragung über ein IPv4-Netzwerk müssen noch der Overhead durch verschiedene höhere Protokollschichten berücksichtigt werden:

IPv4	20 Byte
TCP	20 Byte
TLS 1.3 (in üblicher Konfiguration)	22 Byte
WebSocket (für Payloadlänge zw. 126B-65536B)	4 Byte
OCPP-Nachricht	549 Byte
Gesamtes IP-Paket	**615 Byte**

Es ist auch anzumerken, dass die dargestellte csChargingProfiles-Struktur eine ausführlichere Konfiguration enthält, als sie für das reine Herunterregeln der Ladeleistung notwendig wäre. Eine Auswertung der Latenzzeiten für Paketgrößen im Bereich von 1500 Byte enthält damit reichlich Platz für sowohl ausführlichere Ladeprofile als auch zusätzliche Header, wie sie ggf. durch weitere Sicherheitsprotokolle (etwa falls der Zugriff auf das CPMS durch ein VPN geschützt wird) auftreten können.

4.4.2 Reaktionszeit bei Verwendung von SOAP

Wie oben erläutert, existieren wesentliche Unterschiede hinsichtlich der erreichbaren Verzögerung der SetChargingProfile-Nachricht abhängig davon, ob WebSocket oder SOAP genutzt wird. Aufgrund der Nachteile der Verwendung von SOAP und aufgrund einer deutlich aufwendigeren und differenzierter zu betrachtenden Analyse im Fall von SOAP führen wir in dieser Studie keine detailliertere experimentelle Analyse für den Fall, dass SOAP verwendet wird, durch und verweisen stattdessen auf eine Hochrechnung der oben durchgeführten statistischen Messwerte.

Konkret wird die Reaktionszeit in diesem Fall von der für die Herstellung einer sicheren Verbindung notwendige Anzahl an Roundtrips zwischen Ladestation und CPMS dominiert, die, wie oben erläutert, für einige Konfigurationen beträchtlich sein kann. Unvermeidbar ist ein Roundtrip zur Herstellung der TCP-Verbindung. Im erstrebenswerten Fall einer TLS-gesicherten Verbindung, sind außerdem zwei zusätzliche Roundtrips für TLS 1.2, oder ein zusätzlicher Roundtrip für TLS 1.3, notwendig. Während TLS 1.3 in der Lage ist, zusätzliche Roundtrips für die Verbindungsherstellung auf 0 zu reduzieren, kann dies (siehe oben) Sicherheitsprobleme nach sich ziehen. Wird HTTP-Authentifizierung genutzt, kann

es, wie im OCPP-Standard dargestellt, implementierungsabhängig außerdem sein, dass der erste Request ohne Authentifizierungsdaten gesendet wird und erst beim Erhalt einer 401-Fehlerrückmeldung die zur Realm passenden Zugangsdaten mitgesendet werden. Jeder dieser Roundtrips führt, wie oben dargestellt, bei 2G-Anbindung zu einer zusätzlichen Verzögerung von zumindest 0,6s.

4.4.3 Antwortzeit

Wie oben erwähnt, ist es nicht nur die Zeitspanne interessant, bis die Ladestation mit Leistungsreduktion reagiert, sondern auch die Zeitspanne bis das CPMS von der erfolgreichen Leistungsreduktion informiert wird, kann von Interesse sein. Unabhängig davon, ob die SOAP- oder WebSocket-Variante von OCPP genutzt wird, wird ein SetChargingProfile-Request mit einer entsprechenden Confirm-Nachricht beantwortet.

Da diese Antwortnachricht von geringer Größe ist, können die oben genannten Roundtrip-Messwerte als (worst case) Abschätzung der Zeit bis zum Empfang der Antwortnachricht herangezogen werden. Es ist jedoch fraglich, inwieweit eine Erfolg-signalisierende Antwort tatsächlich als tatsächlich erfolgende Leistungsreduktion interpretiert werden darf. Eine bessere Einschätzung erlauben MeterValue-Nachrichten, wie sie periodisch von der Ladestation übermittelt werden. Da das Intervall, mit dem MeterValue-Nachrichten übermittelt werden jedoch aus regulatorischen Gründen bei mindestens 15 Minuten liegt, können diese Nachrichten jedoch nicht für den Kontrollprozess genutzt werden, da hier automatisiert Entscheidungen im Sekundenbereich getroffen werden müssen. Hinsichtlich eines Übertragungsintervalls von 15 Minuten sind Paketlaufzeiten für periodisch übermittelte Messwerte jedenfalls ohne Relevanz.

5 Detaillierte Sicherheitsanalyse

Die generischen Sicherheits- und Leistungs-Analysen der bisherigen Kapitel werden in diesem Kapitel mit den konkreten Anwendungsfällen zusammengeführt, um konkrete Bedrohungen zu isolieren, die eine mögliche Regelung der Leistung privater Ladestationen durch den CPO verursachen kann. Weiters wird die jeweilige Verzögerung auf Kommunikationsnetzebene berechnet, als Anhaltswert und untere Schranke für die möglichen Verzögerung bei der Steuerung der Ladestation mit dem jeweiligen Protokoll.

5.1 Regelung der Ladeleistung mit OCPP-S

Das Sequenzdiagramm in Abbildung 19 zeigt die Leistungsregelung privater Ladestation durch den CPO in der Annahme einer bereits vorkonfigurierten und in Betrieb genommenen Ladestation mit TLS Client-Zertifikaten. Im Anlassfall (Überlastsignal, Nachricht 1.0 in Abbildung 19) muss der CPO die Möglichkeit haben, IP-Pakete an die evtl. sich hinter einem NAT befindliche Ladestation zu senden (möglich wäre z.B. Port Forwarding vom NAT o.ä.). In Mobilfunknetzen wird vorher notwendigerweise noch ein Träger (Carrier, Nachricht 1.1.) aufgebaut und verursacht zusätzliche Verzögerung (siehe Messergebnisse in Kapitel 4.3). Anschließend wird die TCP/IP Verbindung erstellt (Syn/SynAck/Ack) sowie die TLS-Verbindung aufgebaut (insgesamt mindestens 3 Runden für Nachrichten 1.2 bis 1.7).

Anschließend kann das CPMS das gewünschte Ladeprofil (Nachricht 1.8) als SOAP/XML Nachricht übermitteln und die Ladestation darauf antworten (Nachricht 1.10).

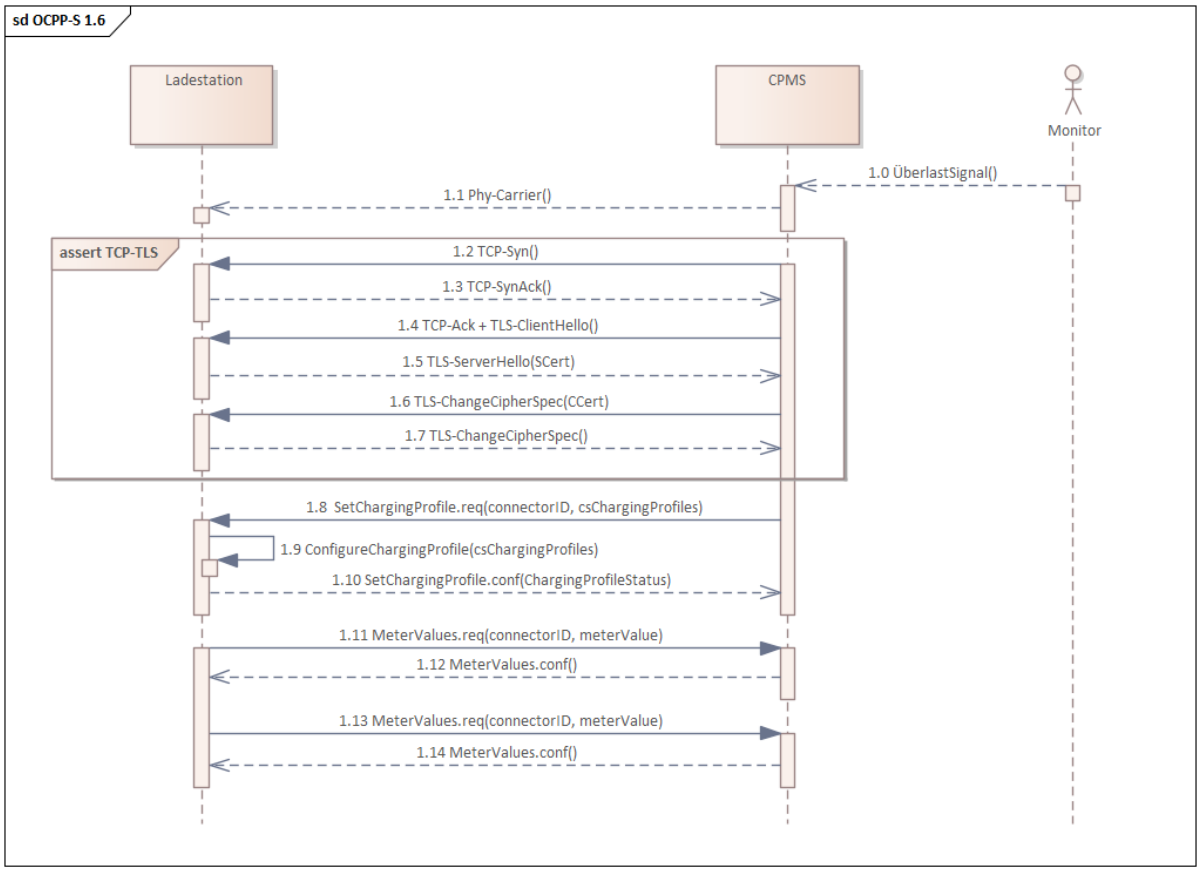

Abbildung 19: Regelung der Leistung einer Kund_innen-Ladestation durch den CPO bzw. CPMS mittels OCPP-S (SOAP/XML): Im Anlassfall (d.h. Bedarf der Regelung) hoher Aufwand und Zeitverzögerung für Verbindungsaufbau. Weiter muss das CPMS in der Lage sein, jederzeit IP-Pakete zur Ladestation der Kund_innen (evtl. hinter einem NAT!) zu senden!

Eine zusätzliche Herausforderung ist, dass die OCPP-Nachricht SetChargingProfile.conf() nur einen Statuswert zurückliefert (Accepted/Rejected/NotSupported). So kann der CPO nie sicher sein, ob und wann das Kommando bei dem Rückgabewert „Accepted“ tatsächlich durchgeführt wurde. Aus diesem Grund sollte als Vorschlag der Studienautor_innen die Ladestation (im Abstand von einigen Sekunden) zwei zusätzliche MeterValues OCPP-Nachrichten absenden, um dem CPMS bzw. CPO eine Rückmeldung über die tatsächlich verbrauchte Leistung zu liefern. Diese Änderung erfordert möglicherweise eine Aktualisierung der Firmware der Ladestation.

Nachteile OCPP-S (vergleiche auch mit Kapitel 3.5.4)

1. Overhead für Verbindungsaufbau bei Notwendigkeit der Leistungsregelung.
2. Ladestation wird als HTTP Server betrieben – demzufolge besteht die Notwendigkeit eines signierten Server-Zertifikats für jede Ladestation.
3. Binden eines HTTP Server Zertifikats an Servernamen, die in vielen Fällen privaten IPv4-Adressen entsprechen.

5.2 Regelung der Ladeleistung mit OCPP-J

Das Sequenzdiagramm in Abbildung 20 beschreibt den Aufbau einer TLS-gesicherten Websocket-Verbindung und die Ladestations-Regelung durch den CPO bzw. durch dessen CPMS. Details zu OCPP-J wurden bereits in den Kapiteln 3.5.1 bzw. 3.5.5 erläutert.

Im Gegensatz zu OCPP-S wird bei OCPP-J die Verbindung immer von der Ladestation zum CPMS aufgebaut. Nach TCP und TLS Verbindungsaufbau wird über HTTP auf das WebSocket Protokoll umgeschaltet. Die Verbindung wird mit KeepAlive-Nachrichten aufrecht erhalten, so dass das CPMS

über die bidirektionale Verbindung jederzeit Befehle an die Ladestation senden kann (selbst über NAT-Grenzen hinweg). Im Bedarfsfall muss das Mobilfunknetz u.U. noch einen Datenträger aufbauen bevor das CPMS die Befehle zur Konfiguration des Ladeprofils an die Ladestation senden kann.

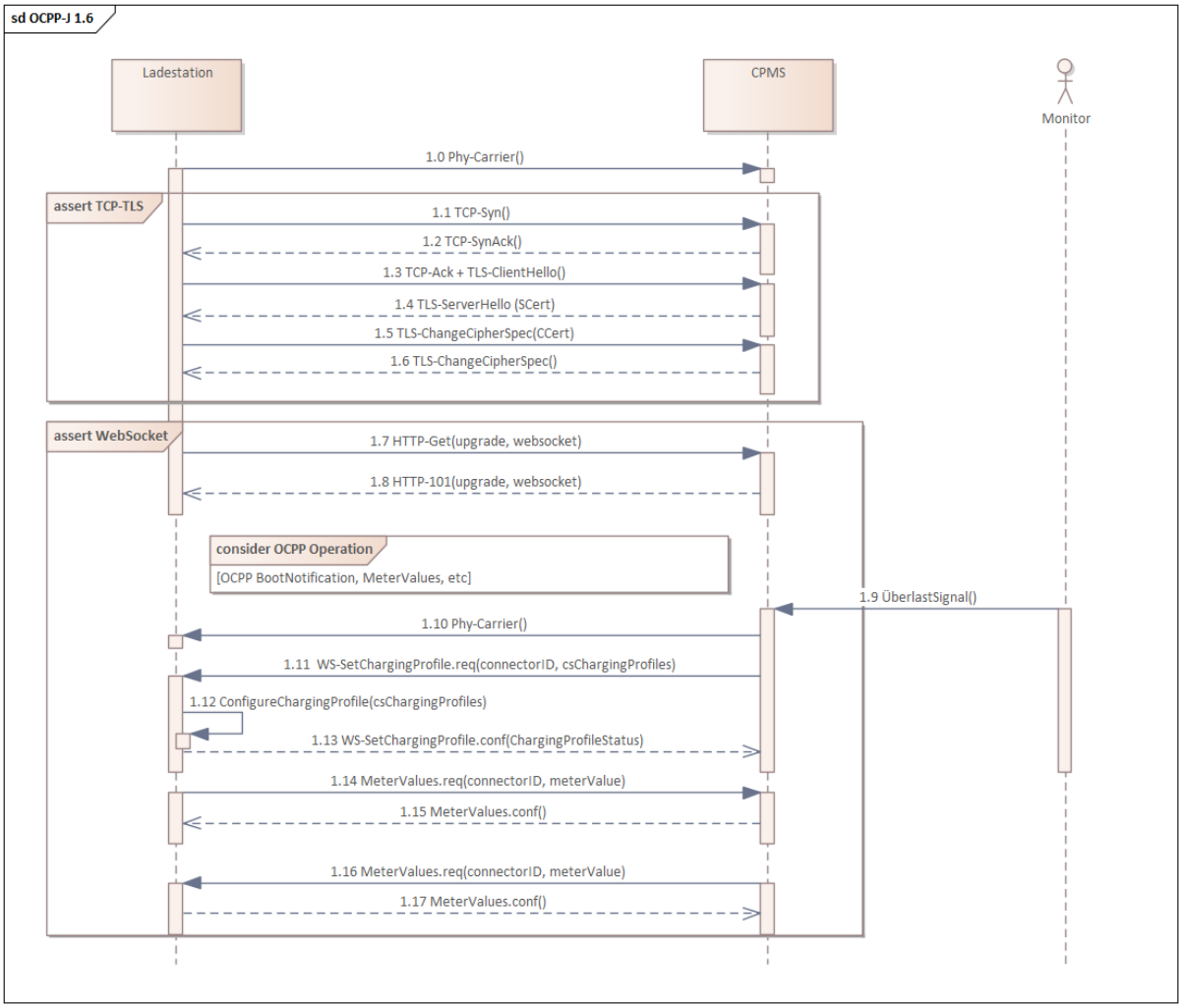

Abbildung 20: Regelung der Leistung einer Kund_innen-Ladestation durch den CPO mittels OCPP-J (JSON/WebSockets). Verbindungsaufbau TCP/TLS (1.2) erfolgt zuerst, anschließend wird mit den dafür vorgesehenen HTTP Headern auf das WebSocket Protokoll umgeschaltet. Anschließend kann das CPMS über diese bidirektionale Verbindung auf die Ladestation zugreifen.

5.3 Kategorisierung der Angriffe

Der folgenden Analyse zugrunde liegen die bereits in Kapitel 3.4 erwähnten Annahmen bezüglich der Fähigkeiten der Angreifer, sowie Möglichkeiten und Sicherheitsmängel in der Fernsteuerung der Ladestationen.

5.3.1 Kritische Einschränkungen in der Funktionalität und Sicherheit

Als kritisch erachtet bzw. betrachtet werden die bereits in Kapitel 3.4.3 gelisteten vier Einschränkungen der Funktionalität und Sicherheit bzw. Privatsphäre, die der Übersichtlichkeit halber an dieser Stelle nochmals wiederholt werden:

1. Ein Angreifer kann die notwendige Regelung von Ladestationen durch den CPO erschweren, stören oder unterbinden
2. Ein Angreifer kann aufgrund von Sicherheitslücken Ladestationen übernehmen und regeln

3. Erschwerend: ein Angreifer erreicht die Einschränkung gemäß Punkt (1) und (2) für eine große Anzahl von Ladestationen
4. Ein Fernzugriff auf die Ladestation durch Angreifer oder CPO gefährdet die Privatsphäre der Kund_innen.

5.3.2 Methode und Angriffsziel

Auf technischer Ebene realisieren können Angreifer die im vorigen Kapitel genannten Einschränkungen durch folgende Methode bzw. Vorgangsweise:

1) Angriffe auf die **Ladestation (**bzw. **Kund_innen)**
2) Angriffe auf das **CPMS** (bzw. den **CPO**)
3) Angriffe auf die **Kommunikation Ladestation – CPMS**
4) Gefährdung der **Privatsphäre von Kund_innen**

Zudem können Kombinationen dieser Methoden zum Einsatz kommen.

5.3.3 Positionierung des Angreifers

Der Angreifer kann dabei an folgenden Orten (entlang des Kommunikationspfads Ladestation-CPMS) positioniert sein und, davon abhängig, unterschiedliche Angriffs- bzw. Eingriffsmöglichkeiten haben:

1) **LAN der Kund_innen:** als plausible Annahme, z.B. über einen mit Malware infizierten PC und der Kompromittierung der Netzkomponenten der Kund_innen wie z.B. DSL- oder WLAN-Router.
2) **Kommunikationsnetz des CPO:** als wenig plausible Annahme, die dennoch behandelt wird – Stichwort „vertrauenswürdige Kommunikationsnetz-Pfade“).
3) Im **Internet** am Kommunikationspfad: als typischer Fall, z.B. bei Infektion eines Routers am Pfad.
4) **Kompromittierte Ladestation:** Fall wird in der Diskussion behandelt; festgehalten werden muss aber, dass eine kompromittierte Ladestation dem Angreifer ggf. vollständige Kontrolle über Ladevorgänge, Kommunikation und Verhalten dieser Ladestation ermöglicht.
5) **Kompromittiertes CPMS:** Eine vollständige Übernahme des CPMS durch einen Angreifer bedeutet vollständige Kontrolle aller gesteuerter Ladestationen des CPMS – und somit eine Vielzahl von Angriffsmöglichkeiten mit kaum vorhandenen Gegenmaßnahmen.

5.3.4 Zeitpunkt und Dauer des Angriffs

Gesondert betrachtet werden müssen mögliche Angriffe in unterschiedlichen Phasen der Inbetriebnahme bzw. im Betrieb der Ladestation, da in diesen Phasen möglicherweise unterschiedliche Sicherheitsannahmen bzw. -assoziationen zwischen Ladestation und CPMS (bzw. Kund_innen und CPO) gelten:

1) Bei der **Herstellung der Komponenten** (Ladestation oder CPMS, klassische Supply-Chain-Angriffe, somit herstellerspezifisch und außerhalb des Umfangs der Studie)
2) **Vor und während der Inbetriebnahme der Ladestation** (persistente Kompromittierung):
    a. Bootstrapping als erfolgsversprechende Angriffsmöglichkeit
    b. Ladestations-IDs, Passwort- und/oder Zertifikatsverteilung, Master-Keys, usw. als Schwachstelle im Initialisierungsprozess
    c. Anmeldeprozess der Ladestation beim CPMS
3) **Nach erfolgreicher Inbetriebnahme der Ladestation** (persistente Kompromittierung):
4) **Während des operativen Betriebs**, d.h. während der Steuerung der Leistung von Ladestationen bei Kund_innen durch den CPO (transiente Kompromittierung):

5.3.5 Relevante Protokolle

Betroffene betrachtete Protokolle und Angriffsmöglichkeiten sind unter anderem:

1) **OCPP-S 1.6, OCPP-J 1.6 und OCPP-J 2.0.1** sind die relevanten Protokolle, mittels derer ein CPO eine Ladestation steuern kann.
2) **TCP/TLS** baut eine sichere Verbindung auf Transportebene auf, deren Vorhandensein Voraussetzung für den sicheren Betrieb von OCPP ist. Mögliche Angriffspunkte sind z.B. fehlende oder kompromittierte Server-Zertifikate, Client-Zertifikate, und/oder deren Gültigkeit.
3) Das Domain Name System (**DNS)** wird standardmäßig ungesichert über UDP übertragen und kann von MitM mit geringem Aufwand manipuliert werden (im Werte- und Zeitbereich)
4) Eine Zeitsynchronisation mittels des Network Time Protocol (**NTP)** wird häufig eingesetzt, um die Zeit der Ladestation an die globale Uhrzeit anzugleichen. NTP ist standardmäßig ungesichert und kann von MitM manipuliert werden (im Werte- und Zeitbereich).
5) Sonstige: Bei einigen generischen Angriffsarten können Angreifer verschiedene, dafür geeignete Protokolle einsetzen (z.B. DNS oder TCP Syn für DoS oder DDoS). Angriffe über Protokolle niedrigerer Schichten wie z.B. Adress-Spoofing-Angriffe mittels des Address Resolution Protokolls sind gängige Praxis und können bzw. müssen über höhere Protokollebenen (z.B. Zertifikate o.ä.) ausgeschlossen werden. D.h. auf IP-Ebene kann der Angreifer die IP-Adresse einer Ladestation annehmen und damit kommunizieren, aber er besitzt die notwendigen Zertifikate nicht, um sich auf Anwendungsebene zu authentifizieren.

5.4 Sicherheitsbeurteilung der Anwendungsfälle

Die in Kapitel 3.2 entwickelten Anwendungsfälle werden in der Folge bezüglich möglicher Angriffsmöglichkeiten analysiert. Ausgehend von der Beschreibung von generischen Angriffsmöglichkeiten, die für mehrere Szenarien anwendbar sind, werden die spezifischen Bedrohungen für die einzelnen Anwendungsfälle entwickelt.

5.4.1 Generische Angriffsmöglichkeiten

Die folgenden Angriffe sind bei mehreren der folgenden Anwendungsfälle zutreffend. Sie werden daher eingangs detailliert und die Anwendungsfälle referenzieren in der Folge darauf.

5.4.1.1 OCPP ohne (oder unzureichend) TLS-gesicherter Kommunikation

OCPP implementiert weder in der JSON/Websocket Variante (OCPP-J 1.6 bzw. 2.01) noch in der SOAP/XML Variante eigene Sicherheitsmaßnahmen. Eine Steuerung der Kund_innen-Ladestation durch den CPO muss aufgrund der in Kapitel 3.5 (3.5.1 - 3.5.6) beschriebenen Argumente zwingend eine TLS 1.2 oder 1.3 Verbindung verwenden um die Vertraulichkeit und Integrität der Daten sowie die Authentifizierung der Kommunikationspartner sicherzustellen. Bezogen auf die OCPP-Sicherheitsprofile (siehe Kapitel 3.5.3, bzw. Tabelle 2) sind die OCPP-Profile „TLS with Basic Authentication“ oder „TLS with Client-Side Certificates“ eine unbedingte Voraussetzung für eine Steuerung gemäß dem in Abbildung 20, Kapitel 5.2 dargestellten Sequenzdiagramm. Desgleichen müssen ausschließlich geeignete, sichere Cipher-Suiten und TLS-Konfigurationen verwendet werden. Notwendige Mindestvorgaben beinhalten u.a. die Vorgaben und Anforderungen des OCPP-Standards unter A00.FR.301-A00.FR.324 und A00.FR.401-A00.FR.429 für OCPP 1.6 im Security Whitepaper V2 [46] bzw. A00.FR.301-A00.FR.323 und A00.FR.401-A00.FR.424 im OCPP 2.0.1 Standard [48]. Nach Abgabe dieser Studie veröffentlichte Erkenntnisse von Standardisierungs- und Sicherheitsorganisationen müssen ebenfalls berücksichtigt werden.

Angriffsvektor: Ohne TLS-Verschlüsselung, bei Verwendung ungeeigneter TLS-Versionen oder unsicherer Ciphers, oder bei Kompromittierung der Zertifizierungskette (Kompromittierung von Zertifikats-Stores in Ladestation und/oder CPMS, Kompromittierung von Zertifikats-Widerruf, usw.) kann ein Angreifer, wie in Kapitel 3.5 beschrieben, die Inhalte der Steuerbefehle in den OCPP-Datenpaketen beliebig modifizieren. Somit kann ein Angreifer falsche Werte bei Ladeprofilen oder Ladezeitpunkten einfügen und hat damit vollständige Kontrolle über die Ladestation.

Anforderung: Größte Herausforderung ist eine fehlende (bzw. nicht in der Praxis einsetzbare) Standardisierung für Verwendung von OCPP-S mit TLS, sowie zeitlicher Overhead beim Verbindungsaufbau mit OCPP-J – vor allem bei langsamen und unzuverlässigen 2G Netzen. Für eine gesicherte Steuerung der Ladestation durch einen CPO ist die ausschließliche Verwendung von OCPP-Profile 2 oder 3 sowie die Verwendung von TLS 1.2 oder 1.3 unbedingte Voraussetzung (beschrieben in OCPP 2.0.1 sowie in OCPP-J 1.6 Security WhitePaper). Weiters sind ausschließlich Cipher zu verwenden, die zum Zeitpunkt des Betriebs als sicher gelten (ausgehend von den oben erwähnten Anforderungen der OCPP Standards sowie aktuellen Vorgaben von Instituten wie NIST [52], ENISA [53], IETF, usw.)

5.4.1.2 Unzulässige TLS-Version

Nach Verabschiedung der gültigen OCPP-Standards (OCPP 1.6 bzw. 2.0.1) hat die IETF, wie in Kapitel 3.5.2 beschrieben, die TLS-Versionen 1.0 und 1.1 in einem formalen Dokument [45] als nicht mehr zulässig kategorisiert. Die Begründung dafür ist Angreifbarkeit und mögliche Erhöhung der Angriffsfläche von Systemen bei Verwendung der alten TLS-Versionen und deren als verpflichtend vorgesehenen Algorithmen – insbesondere die Anfälligkeit für sogenannte „Downgrade“-Angriffe. Behörden und Industrieforen haben in der Folge aufgrund möglicher Sicherheitsmängeln und -gefährdungen die Nutzung von TLS in den Versionen 1.0 und 1.1 explizit verboten.

Angriffsvektor: Die Anmerkungen im Security WhitePaper zu OCPP 1.6 (u.a. in Kapitel 2.4.1, A00.FR.312) erlauben aus Gründen der Rückwärtskompatibilität die Nutzung von TLS 1.0 und 1.1. Angreifer könnten beim Zulassen von TLS 1.0 oder 1.1 vorgeben, keine höhere TLS-Version zu unterstützen um den Einsatz kompromittierbarer Verschlüsselung zu erzwingen.

Anforderung: Die Schlussfolgerungen von RFC 8996 [45] müssen berücksichtig werden: die Unterstützung der beiden TLS-Versionen 1.0 und 1.1 ist nicht zulässig. OCPP 2.0.1 schreibt bereits TLS 1.2 als Mindestanforderung fest (Kapitel 1.3.5, A00.FR.313).

5.4.1.3 TLS ohne Client-seitige Zertifikate

TLS sieht, wie in Kapitel 3.5.2 beschrieben, verpflichtende Server-Zertifikate vor (selbstverständlich mit vertrauenswürdigem, nicht kompromittiertem Aussteller der Zertifikate und entsprechenden Zertifikats-Ketten). Client-seitige Zertifikate sind gemäß TLS-Standardisierung optional, jedoch notwendig um die Authentizität des Clients sicherzustellen. Für CPO-gesteuerte Ladestationen werden Client-Zertifikate aus Sicherheitsgründen empfohlen. Die Steuerung könnte jedoch, wenn in der Folge beschriebene Vorbedingungen erfüllt sind, auch in Abwesenheit von Client-Zertifikaten sicher implementiert werden.

Angriffsvektor: Angreifer können, falls Client-seitige Zertifikate nicht verpflichtend sind, gültige TLS-Verbindungen zum CPMS aufbauen und somit Ressourcen des CPMS verbrauchen. Bei Verwendung von Malware können Angreifer dadurch (unter Missbrauch der Ressourcen von nicht beteiligten Dritten, z.B. über Botnetze und Verwendung von kompromittierten PCs) effiziente DDoS Angriffe auf den CPMS starten. Der erfolgreich TLS-Aufbau von Angreifern bedeutet jedoch nicht notwendigerweise, dass sich Angreifer als MITM zwischen Ladestation und CPMS einschleusen können. Bedingung dafür ist, dass (a) die Ladestation das gültige Server-Zertifikat des CPMS validieren kann und (b) die Ladestation über einen dem Angreifer unbekannten und nicht erratbaren bzw.

berechenbaren Schlüssel zur Authentifizierung beim CPMS bzw. CPO verfügt. Sind die Bedingungen (a) und (b) erfüllt, ist sichergestellt, dass ein Angreifer (trotz fehlender Client-Zertifikate) sich auf OCPP-Ebene **nicht** beim CPMS als Ladestation von Kund_innen anmelden kann. Zur Begründung: die Ladestation kann die Authentizität des CPMS beim Aufbau der TLS-Verbindung anhand des gültigen Server-Zertifikats verlässlich feststellen. Der Angreifer kann sich somit gegenüber der Ladestation **nicht** als CPMS ausgeben und somit auch nicht als MITM agieren und nicht an den Schlüssel der Ladestation gelangen. Der CPMS fordert nach OCPP-Aufbau von der Ladestation den geheimen Schlüssel an. Anfrage und Austausch erfolgt geschützt durch die vorab erstellte TLS Verbindung. Da der Angreifer diesen Schlüssel nicht hat und auch keine Möglichkeit besitzt, die Ladestation zur Herausgabe des Schlüssels zu bringen, kann er sich nicht statt der legitimen Ladestation anmelden.

Anforderung: Herausforderung ist im Idealfall (Verwendung von Client-seitigen Zertifikaten) die sichere, vertrauliche Verteilung bzw. Installation der Client-Zertifikate – idealerweise durch den Hersteller der Ladestation – sowie deren langfristige Wartung. OCPP 2.0.1 sowie das Security WhitePaper für OCPP-J 1.6 sehen Update-Mechanismen vor. Zertifikat-Updates müssen ausnahmslos über (TLS-gesicherte) Verbindungen erfolgen (d.h. Profile 2 oder 3). Falls keine Client-Zertifikate verwendet werden (d.h. bei Verwendung von OCPP Security Profile 2), muss durch den Hersteller (a) ein eindeutiger, für Angreifer nicht errat- bzw. berechenbarer Schlüssel auf den Ladestationen installiert werden, gemeinsam mit (b) allen notwendigen Root- und Intermediate-Zertifikaten, damit die Ladestationen beim Aufbau der TLS-Verbindung die Gültigkeit von Server-Zertifikaten des CPMS verlässlich überprüfen können.

5.4.1.4 Angreifbare Zeitsynchronisation und TLS

Voraussetzung für die Funktionalität bzw. Verifikation von Zertifikaten ist eine hinreichende Zeitsynchronisation von Ladestation und CPMS sowie eine ausreichend lange Gültigkeit von Zertifikaten. Hinreichend bedeutet, dass die lokale Zeit der genannten Systeme innerhalb der Gültigkeit der Zertifikate liegt. Batteriegepufferte Uhren in Ladestationen sind ggf. nicht zeitsynchron und die Abweichung zu der globalen Zeit ändert sich mit der Lagerzeit der Ladestation bis zum ersten Einsatz.

Angriffsvektor: Für den Aufbau einer gültigen TLS-Verbindung muss die Ladestation hinreichend zeitsynchron sein. Die gültige TLS-Verbindung ist allerdings auch Voraussetzung für die Zeitsynchronisation der Ladestation durch den CPMS mittels OCPP (initial im BootNotification.conf, anschließend über Heartbeat.conf). Ist eine Ladestation nicht (mehr) hinreichend zeitsynchron für die Validierung der Zertifikate, kann keine gültige TLS Verbindung aufgebaut werden. Hersteller setzen als Alternative der Zeitsynchronisation auf das Network Time Protocol (NTP) – und bauen damit schwerwiegende Sicherheitsgefährdungen ein. NTPv4 ist in den gängigen Implementierungen unverschlüsselt und nicht signiert (Network Time Security, NTS ist komplex und derzeit nicht im Feld implementiert)**.** Angriffe auf die NTP-Zeitsynchronisation sind daher (sowohl im Wertebereich als auch im Zeitbereich) für MitM-Angreifer problemlos machbar. Aus Gründen der Sicherheit muss daher von der Verwendung von NTP für die Zeitsynchronisation der Ladestationen abgeraten werden! Während eine (grobe) Zeitsynchronisation der Ladestation mit OCPP nach einer erstmaligen Inbetriebnahme und sicherer TLS-Verbindung ausreichend ist, können Angreifer eine permanente Zeitsynchronisation der Ladestation mit NTP jederzeit für Angriffe missbrauchen.

Anforderung: Notwendig für einen sicheren Betrieb der Ladestation ist das Herstellen einer hinreichenden Zeitsynchronisation der Ladestation bei deren ersten Inbetriebnahme. Eine batteriegepufferte Uhr sollte auch bei langjähriger Lagerung der Ladestation die notwendige Genauigkeit haben – Herausforderung ist eher die Gültigkeit der auf der Ladestation gespeicherten, signierten Zertifikate (meist nur ein Jahr gültig). Deutlich einfacher und sicherer als NTP ist z.B. das

explizite Setzen der (ungefähren) aktuellen Zeit der Ladestation durch Techniker_innen oder Kund_innen bei der Installation oder Erstkonfiguration.

Nicht empfohlen, aber technisch vertretbar wären einige andere Optionen (genauer: Notlösungen) um eine sichere TLS-Verbindung bei der ersten Inbetriebnahme der Ladestation zu ermöglichen:

1. Standard-Uhrzeit bei erstmaliger Inbetriebnahme: die Ladestation könnte nach einem Reset mit definierter (falscher) Standard-Uhrzeit starten (z.B. 1.1.1970) und die Zertifikate mit entsprechender Gültigkeitsdauer gespeichert haben. Wenn der CPMS auch passende Server-Zertifikate bereitstellt, kann eine TLS-Verbindung aufgebaut werden um Aktualisierungen von Zertifikaten, Firmware, usw. der Ladestation über OCPP durchzuführen. Herausforderung ist hierbei für das CPMS, den für die Zeitsynchronisation in BootNotification.Conf() des CPMS entsprechend Zeitstempel bis zum erfolgreichen Abschluss der Aktualisierungen zurückzuhalten (d.h. Datum z.B. 1.1.1970). Nach Abschluss der Aktualisierungen setzt das CPMS die aktuelle Zeit auf der Ladestation und erzwingt anschließend ein Reboot (mit nun gültiger Uhrzeit und Zertifikaten).
2. Ignorieren der Anfangszeit der Gültigkeit von Zertifikaten: wenn angenommen wird, dass die Uhrzeit der Ladestation deutlich früher ist als die tatsächliche Zeit (z.B. 1.1.1970 nach Reset) könnte die TLS-Implementierung in der Ladestation so modifiziert werden, dass sie die Zertifikate auf Gültigkeit prüft, jedoch (beim ersten Booten) den Anfangszeitpunkt der Gültigkeitsdauer von Zertifikaten ignoriert. Sofern sichergestellt werden kann, dass die Root- und Intermediate-Zertifikate der Zertifizierungsstelle nicht kompromittiert sind bzw. in der Zwischenzeit widerrufen wurden, kann mit dieser Methode auch eine sichere TLS-Verbindung aufgebaut werden. Selbstverständlich nur um aktuelle Zertifikate und Firmware-Images einzuspielen und nach einem anschließenden Setzen der Uhrzeit der Ladestation das Default-Verhalten der TLS-Implementierung wieder zu aktivieren (d.h. Zertifikate müssen innerhalb der Gültigkeitsdauer liegen um akzeptiert zu werden).

5.4.1.5 Domain Name System (DNS) Angriffe

DNS bildet Namen auf Ressourcen ab – z.B. bei Abfrage von Typ A Informationen qualifizierte Hostnamen wie tunamea.tuwien.ac.at auf der bzw. den zugehörigen IPv4 Adresse(n). Derzeit wird DNS großteils unverschlüsselt (UDP Port 53) eingesetzt, verschlüsselte Alternativen wie DNS over TLS (DoT, [54]), DNS over HTTP(S) (DoH, [55]) und DNS Security Extensions (DNSSec, [56]) wurden von der IETF standardisiert, sind aber vor allem im M2M oder IoT Bereich nicht gebräuchlich. Angreifer können daher DNS-Aufrufe von Ladestationen beliebig modifizieren und Aufrufe der Ladestation oder des CPMS auf andere, kompromittierte, Gegenstellen umleiten.

Sofern die Kommunikation Ladestation – CPMS jedoch TLS-verschlüsselt ist und dabei auf beiden Seiten Client- und Server-Zertifikate mit korrekten Zertifikatsketten (certificate chains) verwendet werden, ist bei einer Kompromittierung des DNS zwar eine Fehlfunktion der Lade-Infrastruktur möglich. Die Nachricht des Senders kann aufgrund von Angreifer-modifizierten DNS-Informationen bei einem kompromittierten Empfänger landen, jedoch kann diese kompromittierte Komponente sich weder gegenüber Ladestation noch gegenüber CPMS als deren legitimer Gegenpart ausweisen. Eine steuernde Einschleusung des Angreifers als MitM zwischen Ladestation und CPMS ist bei korrekt funktionierender Zertifikatskette und Verschlüsselung bzw. Integritätsprüfung unwahrscheinlich.

5.4.1.6 Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS) Angriffe

Aufgrund des Einsatzes von TCP als zugrundeliegendes Transportprotokoll (unterhalb von TLS) sind Ladestation und CPMS durch Syn-Flooding-Angriffe gefährdet, die als DoS und DDoS ausgeführt werden können.

Angriffsvektor: Angreifer können diese bekannte Anfälligkeit von TCP missbrauchen um Ressourcen von Ladestation oder CPMS vollständig auszulasten und deren Speicher zu verbrauchen. Firewalls und passende Regeln können und müssen eingesetzt werden, um das Risiko von DoS und DDoS zu minimieren.

Herausforderung: Entscheidende Faktoren in der Abwehr von (D)DoS sind (a) die Positionierung des Angreifers sowie (b) die Möglichkeit, IP-Adressen von legitimen Sendern in Firewalls einzuschränken.

Anforderung: Aufgrund des Einflusses der Positionierung des Angreifers werden die Details und Gefährdungen bzw. Anforderungen für sichere Ladestations-Steuerung jeweils beim entsprechenden Anwendungsfall besprochen. Grundsätzlich ist festzuhalten, dass (D)DoS Angriffe in vielen Fällen nicht auszuschließen sind. Empfehlenswert ist daher eine ausführliche Netzplanung und das Einrichten von Default-Lastprofilen für den Fall, dass die Ladestation das CPMS nicht kontaktieren kann. In diesem Fall soll die Ladestation umgehend auf das Default-Lastprofil entsprechend den Vorgaben zurückstellen, bis das CPMS wieder erreichbar ist.

5.4.1.7 Firmware-Updates von Ladestationen

In OCPP 1.6. wird im normativen Kapitel 8 (Firmware and Diagnostics File Transfer) die Verwendung vom File Transfer Protocol (FTP) für Firmware-Updates aufgrund höherer Effizienz empfohlen. Weiters wird die Signierung des Firmware-Images (nur) empfohlen.

Angriffsvektor: Dieser Empfehlung steht entgegen, dass FTP ausschließlich Klartext-Übertragung von Kontrolldaten (einschließlich Zugangsdaten und Passwort) und Daten unterstützt. Passwörter können daher durch Angreifer ausgespäht werden und Firmware-Images (in Abwesenheit von Signaturen) modifiziert werden, ohne dass die Ladestation das merkt.

Anforderung: Eine eindeutige, nicht kompromittierbare Signatur des Firmware-Images durch den Hersteller mit Möglichkeit der verlässlichen Prüfung in der Ladestation ist als verpflichtend vorzusehen (Signatur und Firmware-Update gemäß OCPP 2.0.1 bzw. Security WhitePaper OCPP-J 1.6). Von der Nutzung von FTP für die Übertragung der Firmware-Updates der Ladestationen wird aus den oben genannten Gründen abgeraten.

Zwei Gründe wurden von Industrievertretern als Argument für die notwendige Nutzung von FTP für die Übertragung der Firmware-Images genannt: (a) effiziente(re) Datenübertragung (binäre Dateien, dedizierter Datenkanal) und (b) die Möglichkeit des Wieder-Aufsetzens nach Übertragungsfehlern. Beide Argumente zielen darauf ab, große Firmware-Images bei niedrigen Übertragungsraten und schlechter Funkversorgung zur Ladestation zu übertragen. Typisches Beispiel sind schlechte, fehleranfällige 2G Anbindungen von Ladestationen in ländlichen Bereichen oder in Gebäuden/Tiefgaragen. Für Punkt (a) gehen die Autor_innen dieser Studie davon aus, dass, angesichts der für FTP vorgesehenen Klartext-Authentifizierung und der beiden aufzubauenden TCP-Verbindungen (Kontrolle, Daten) HTTP über TLS (HTTPS) in der Praxis mit FTP vergleichbare Transferleistung erbringt. Bezüglich Punkt (b) bietet HTTPS standardisierte Möglichkeiten des Wieder-Aufsetzens nach Fehlern bzw. Unterbrechungen mittels HTTP-Erweiterungen in Clients und Servern („Range Requests“, standardisiert in [57], aktualisiert in Kapitel 14 von [58]). Demzufolge gibt es keine technischen Alleinstellungsmerkmale, die eine Verwendung von FTP erzwingen; HTTPS wird für die Übertragung von Firmware-Images zu Ladestationen empfohlen.

Theoretisch möglich ist sogar eine Verteilung der signierten Firmware-Images für Ladestationen über öffentliche FTP-Server ohne jegliche Authentifizierung der Ladestationen. Voraussetzung dafür bzw. Risiko dabei ist, dass die Implementierungen der Ladestation sowohl für FTP-Empfang des Firmware-Images als auch für Prüfung der Herstellersignatur fehlerfrei sein müssen. Ladestationen müssen damit rechnen, dass Angreifer die Firmware-Images modifizieren und Schadcode einschleusen, um ggf.

Schwachstellen in der Implementierung der Ladestation auszunutzen. Diese Sicherheit zu gewährleisten ist deutlich schwieriger als eine Implementierung mit HTTPS-gesicherter Übertragung – Angreifer können mit geringem Aufwand (Änderung eines Bits des übertragenen Firmware-Images genügt) verhindern, dass eine Ladestation das Firmware-Image aktualisiert. Die auf die Übertragung folgende Prüfung der Hersteller-Signatur des Firmware-Images ist jedenfalls in allen beschriebenen Fällen zwingend notwendig.

5.4.1.8 OCPP Security Profile-Update

Gemäß OCPP 2.0.1 und OCPP-J 1.6 Security WhitePaper (jeweils Anforderung A00.FR.005) ist bei OCPP Security Profilen ausschließlich ein Upgrade erlaubt, aber kein Downgrade. Das ermöglicht einen Angriff auf die Verfügbarkeit der Ladestation.

Angriffsvektor: Sollte es einem Angreifer gelingen, ein Profile-Upgrade zu erzwingen, für das die Bedingungen nicht erfüllt sind (z.B. Update von Profile 2, TLS, auf Profile 3, TLS mit Client-Zertifikaten, und Client-Zertifikate sind auf der Ladestation ungültig oder nicht konfiguriert), ist die Ladestation bis zu einem manuellen Eingriff des Betreibers nicht mehr verwendbar (da OCPP kein Profile-Downgrade erlaubt). Die Wahrscheinlichkeit so eines Angriffs ist als eher gering einzuschätzen und setzt (mindestens) eine Kontrolle des Angreifers über die Ladestation voraus (z.B. über kompromittiertes CPMS).

Anforderung: OCPP-Profile-Updates sollten – auch vom CPO – ausschließlich dann durchgeführt werden können bzw. dürfen, wenn alle Vorbedingungen für das höhere Profil erfüllt sind und sichergestellt ist, dass das höhere Profil zu keiner Funktionseinschränkung führt.

5.4.1.9 Privatsphäre von Kund_innen

Die Steuerung und Anbindung der Ladestation an das eigene CPMS erlaubt dem CPO das Erstellen detaillierter zeitlicher Verhaltensprofile von Kund_innen als mögliche Gefährdung der Privatsphäre von Kund_innen.

5.4.2 AF1: Ladestations-Zugriff über Mobilfunk

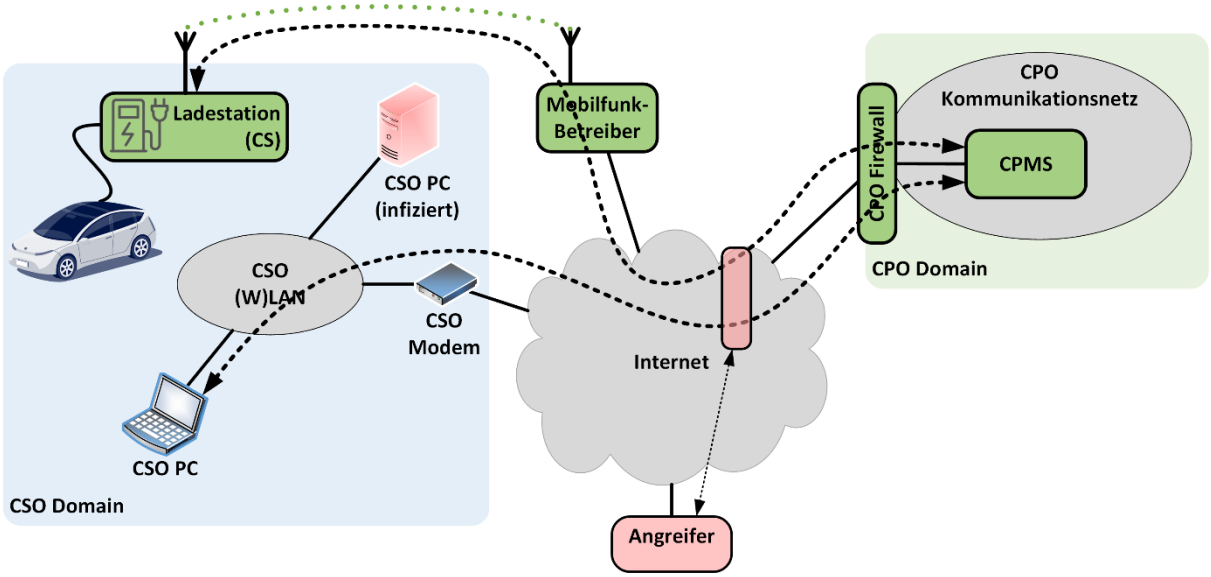

Abbildung 21: Angriffsmöglichkeiten bei (ausschließlicher) Steuerung der Ladestation durch den CPO über Mobilfunk.

Die Sicherheit der Ladeinfrastruktur bei ausschließlichem CPO-Zugriff auf die Ladestation von Kund_innen mittels Mobilfunk (**ohne Anbindung der Station ins Kund_innen LAN**) setzt für die

Sicherheit die Einhaltung der generischen Maßnahmen und Anforderungen gemäß Kapitel 5.4.1 voraus.

Diese Variante hat wesentliche **Vorteile:**

1. **Schutz der Privatsphäre der Kund_innen:** CPOs haben keinen Zugriff auf Kund_innen-(W)LANs, können demzufolge die Ladestation technisch gesehen **nicht** als Jump-Host für das Ausspähen des Kund_innen-(W)LANs verwenden. Das Erstellen von Nutzerprofilen gemäß 5.4.1.9 ist selbstverständlich gegeben und möglich.
2. **Synchronisation der Zugriffe**: Kund_innen greifen ausschließlich über CPO/CPMS Schnittstellen auf die eigene Ladestation zu. Der CPO kann somit die Anforderungen von Kund_innen und ihm selber synchronisieren, d.h. Kompromisse der möglicherweise in Konflikt befindlichen Anforderungen finden. Dieser Single-Point-Of-Access vereinfacht aus technischer Sicht die Konfliktlösung und Ansteuerung bzw. Priorisierung des Zugriffs.
3. **Signifikante Reduktion der möglichen Angriffsfläche (DoS und DDoS, Kapitel 5.4.1.6):** Die Verwendung von privaten Access Point Name (APN)-Angeboten der Mobilfunkbetreiber erlauben die Definition von eindeutigen, fixen IP-Adressen für Ladestationen und CPMS – evtl. sogar in privaten, abgeschotteten IP-Adressbereichen. Technisch möglich ist somit eine Einschränkung des externen Zugriffs auf die Endgeräte (Ladestation und CPMS) mittels Endgeräte-lokaler Firewalls: Auf die Ladestation kann/können ausschließlich die IP-Adresse(n) des CPMS zugreifen, während der CPMS die OCPP-Kommunikation ausschließlich auf die IP-Adressen (vor)registrierter Ladestationen einschränkt. Ergänzend kann der Zugriff auch auf bestimmte zugelassene Protokolle und Ports eingeschränkt werden. Angriffe aus dem Internet werden damit um Größenordnungen schwieriger oder (ohne Kompromittierung von Systemen des CPO) überhaupt unterbunden. Kund_innen müssen zwar eine Möglichkeit des Zugriffs auf die eigene Ladestation haben – typischerweise bietet der CPO dafür ein Web-Interface an. Angriffe auf dieses Web-Interface aus dem Internet sind möglich, aber deutlich besser handhabbar als Angriffe auf eine Ladestation.

Mögliche Nachteile:

1. **Steuerung der Ladestation erfordert funktionale Mobilfunkverbindung:** Die Mobilfunkverbindung ist ein Single-Point-of-Failure: Sofern die Mobilfunkverbindung unterbrochen wird (Störung im Bereich des Mobilfunkbetreibers, Kommunikationsnetz CPO-Mobilfunkbetreiber, Funkversorgung der Ladestation) ist eine Steuerung der Ladestation durch den CPO nicht mehr möglich.
2. **Mobilfunk-Versorgung abgeschirmter Bereiche schwierig:** Herausforderung ist hierbei vor allem die Funkversorgung von abgelegenen Ladestationen sowie von Ladestationen, die in gut abgeschirmten Gebäuden betrieben werden (beispielsweise in gut abgeschirmten Tiefgaragen ohne Mobilfunkempfang). Mögliche technische Lösungen sind mit Kosten verbunden und reichen je nach Fall von Mobilfunk-Repeatern des Mobilfunkbetreibers über Micro-Funkzellen bis zu Empfangsanlagen in anderen Gebäudeteilen und sicheren, dedizierten LAN- bzw. WLAN-Verbindungen zu der Ladestation. Alle diese Lösungen eröffnen jedoch zusätzliche Angriffsflächen, die von Angreifern missbraucht werden können um sich als MitM einzuschleusen. Wie in Kapitel 5.4.1.1 und 5.4.1.2 beschrieben, sind Protokolle wie OCPP, die in Security Profile 2 und 3 TLS Ende-zu-Ende-Verschlüsselung verwenden, von dieser Gefährdung nicht oder nur eingeschränkt betroffen – im Gegensatz zu Protokollen wie DNS oder NTP, die Klartext-Übertragung ohne Sicherung verwenden.
3. **Eingriffsmöglichkeiten des Mobilfunkbetreibers möglich:** Mobilfunkbetreiber können Konfigurationen modifizieren (z.B. Zuordnung von IP-Adressen zu SIM-Karten) und damit die Funktion des Systems gefährden. Auch über Änderungen in der Mobilfunkversorgung (Ändern

von Antennen-Konfigurationen, -Ausrichtungen, unterstützten Technologien wie 2G, 3G, usw.) kann der Mobilfunkbetreiber die Steuerung der Ladestationen verunmöglichen oder erschweren. Hilfreich und notwendig ist jedenfalls ein zusätzlich gesicherter Link (VPN-Tunnel wie z.B. IPsec) zwischen den Kommunikationsnetzen des CPOs und des Mobilfunkbetreibers. Offensichtliche Gefährdung besteht auch bei einer möglichen Kompromittierung von Systemen des Mobilfunkbetreibers durch Angreifer oder nicht vertrauenswürdige Hersteller.

4. **Gefährdung durch Downgrade-Angriffe:** Mobilfunkverbindungen werden durch Verschlüsselung geschützt. Diese Verschlüsselung bietet jedoch aufgrund bekannter Downgrade-Angriffsmöglichkeiten keine Sicherheit (wie in Kapitel 3.5.5.1 detailliert). Bei Protokollen mit TLS-Ende-zu-Ende-Verschlüsselung kann man von einer Sicherheit gegenüber Angriffen im Wertebereich ausgehen (d.h. Modifikation der Daten durch Angreifer sind nicht möglich). Unverschlüsselte Protokolle wie NTP und DNS sowie unverschlüsseltes OCPP sind bei Mobilfunk-Anbindung für Angriffe im Wertebereich sehr wohl anfällig. Weiters können Angreifer als MitM mit technischem Aufwand auch Angriffe im Zeitbereich starten (Zeitsynchronisation über NTP, Verzögerung von Nachrichten, auch wenn TLS-verschlüsselt). Da diese Angriffe gezielt auf jede einzelne Ladestationen erfolgen müssen und jeweils einen hohen technischen Aufwand beinhalten, einschließlich physischer Präsenz vor Ort (IMSI-Catcher für Downgrade), kann diese Gefährdung für großflächige Angriffe weitgehend ausgeschlossen werden.
5. **Notwendigkeit der Isolation:** CPOs können und müssen (mit Unterstützung des Mobilfunkbetreibers) auf technischer Ebene sicherstellen, dass Ladestationen ausschließlich mit dem CPMS und systemrelevanten Geräten wie z.B. DNS-Server, nicht jedoch mit anderen Ladestationen oder dem Internet kommunizieren können. Diese Absicherung wird unter dem Begriff „Intra-APN"-Sicherheit geführt.
6. **Gefährdung durch Diebstahl und Missbrauch der SIM-Karte und/oder des Modems:** Falls es Angreifern gelingt, die SIM-Karte einer angemeldeten Ladestation zu entwenden, können sie die Ladestation „emulieren" um Zugriff auf das CPMS zu erlangen. In der Folge können Schwachstellen des CPMS ausgespäht und für eine mögliche Kompromittierung genutzt werden. Entsprechende Vorsichtsmaßnahmen sind daher für den CPO verpflichtend:
    - **a.** Binden jeder SIM-Karte an das Modem der Ladestation (IMSI-IMEI Verknüpfung) im Backend des Mobilfunkbetreibers mit Alarm bzw. Deaktivierung der SIM-Karte im Fehlerfall. D.h., falls eine SIM-Karte in einem anderen Modem als dem der Ladestation eingesetzt wird, wird die Karte automatisch deaktiviert. Fortgeschrittenen Angreifern wäre jedoch mit entsprechendem technischen Aufwand die Erstellung eines Modems mit der IMEI der Ladestation möglich.
    - **b.** Der CPMS sowie alle von Kund_innen-Ladestationen aus mittels Mobilfunk-Kommunikation erreichbaren Geräte müssen aus Sicht der Kommunikationsnetze gemäß dem Stand der Technik abgesichert werden. Der CPO muss davon ausgehen, dass die Ladestationen von Kund_innen potentiell kompromittiert sind und seine Sicherheitskonfiguration entsprechend auslegen.
    - **c.** Punkte a und b gelten insbesondere für den Fall, dass ein Angreifer Modem und SIM-Karte gleichzeitig aus der Ladestation entwenden kann (z.B. USB-Modem als Dongle mit SIM-Karte, abgesteckt nach Aufschrauben der Station). Aufgrund von bei SIM-Karten im IoT-Bereich typischerweise abgeschalteten PIN-Abfragen der SIM-Karten kann in der Folge der Angreifer das CPMS mit der IP-Adresse der Ladestation kontaktieren. Hauptaugenmerk des CPMS muss sein, dass potentielle Angreifer die Zertifikate und das Schlüsselmaterial von Ladestationen nicht zusätzlich abgreifen können. Der gleichzeitige Diebstahl von SIM-Karte, Modem und Schlüsselmaterial/Zertifikaten einer Ladestation ist äquivalent zu deren vollständigen

Kompromittierung. Auch wenn diese Variante in Einzelfällen denkbar ist: in großem Maßstab ist so eine Aktion für Angreifer sehr aufwändig und daher unrealistisch.

d. Als Sicherheitsmaßnahme gegen den Zugriff Dritter empfiehlt sich eine Absicherung der Ladestation durch den CPO. Komplexere Lösungen um den physischen Zugriff Dritter zu verhindern sind bekannt (z.B. Server, die unbefugte Öffnung erkennen und sofort die gespeicherten Daten löschen) und etabliert aber mit Zusatzkosten verbunden.

7. **Notwendigkeit lokaler Steuerung der Ladestation:** Aufgrund der möglichen hohen Latenzen über Mobilfunk kann eine lokale Laststeuerung der Ladestation notwendig sein um in Fällen lokaler Überlastung innerhalb von Sekundenbruchteilen reagieren zu können. Eine Variante wäre z.B. das sofortige Abschalten bei einem Überlastsignal – das wiederum als mögliche zusätzliche Angriffsfläche für Angreifer verwendet werden könnte.
8. **Betrieb und Folgekosten:** Die Mobilfunkanbindung aller Ladestationen von Kund_innen sowie Verwaltung und Betrieb bedeutet möglicherweise signifikante Zusatzkosten und -aufwand für den CPO. Das übertragene Datenvolumen kann nicht quantifiziert werden, hängt entscheidend von der verwendeten Implementierung und Granularität (i.e., zeitlichen Auflösung) der Steuerung der Ladestationen ab.

Die genannten Vorteile/Nachteile gelten zusätzlich zu den generischen Angriffsmöglichkeiten und Gefährdungen in Kapitel 5.4.1.

Zusammenfassung Zugriff über Mobilfunk (AF1): Die Anbindung über Mobilfunk ist sowohl für CPO als auch für Kund_innen eine Lösung, die unter den analysierten Anwendungsfällen die geringste Angriffsfläche und die meiste Privatsphäre bietet. Nachteilig ist der direkte Kontrollverlust von Kund_innen über ihre Ladestation, die Abhängigkeit von Mobilfunkbetreibern, sowie u.U. Kapazitätseinschränkungen der Mobilfunkverbindung (geringe Datenübertragungsrate, hohe Verzögerung, vor allem bei 2G – siehe Kapitel 4.3). **Wichtig ist festzuhalten, dass die Mobilfunk-Verschlüsselung aufgrund bekannter Angriffsmöglichkeiten keinesfalls als Sicherung angesehen werden kann. Eine zusätzliche Ende-zu-Ende Verschlüsselung (Profil 2 oder 3 von OCPP) ist jedenfalls Voraussetzung für die sichere Steuerung von Ladestationen.**

5.4.3 AF2: Ladestations-Zugriff über das Kommunikationsnetz der Kund_innen

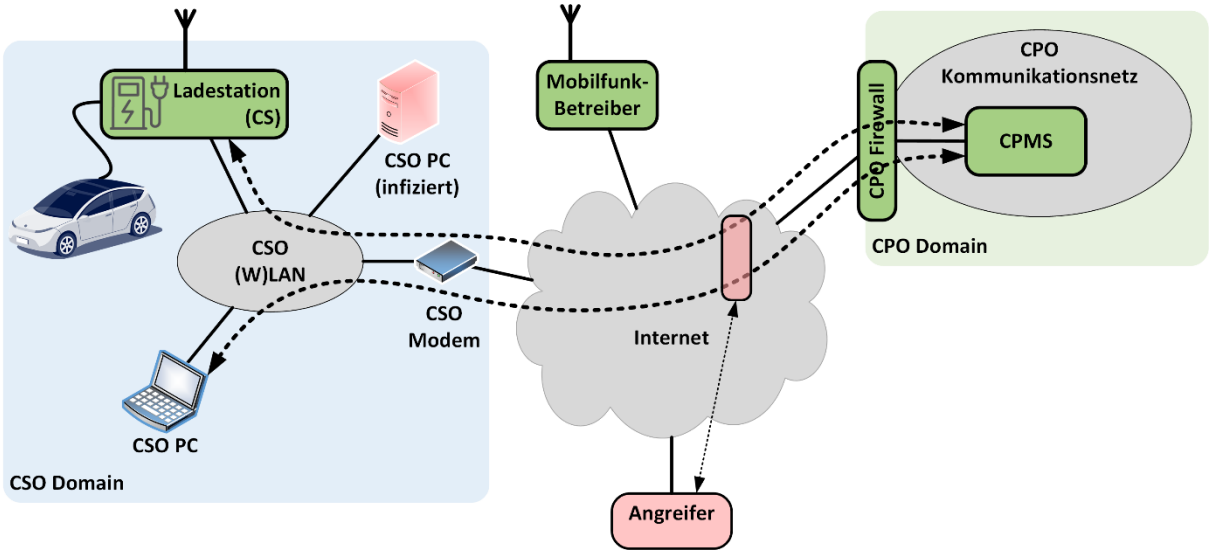

*Abbildung 22: Angriffsmöglichkeiten bei Steuerung der Ladestation durch den CPO über das Kommunikationsnetz der Kund_innen. **Variante a:** Kund_innen haben keinen direkten Zugriff (über WLAN) auf die Ladestation.*

Bei dieser Option greift der CPO mittels Kund_innen-LAN auf die Ladestation zu. Variante a dieses Anwendungsfalls schränkt ein, dass Kund_innen (trotzdem die Ladestation in ihrem LAN oder WLAN hängt) keinen direkten Zugriff auf die Ladestation haben, sondern, wie beim Mobilfunk, über das Web-Interfaces des CPO kommunizieren müssen. Alle generischen Maßnahmen und Anforderungen gemäß Kapitel 5.4.1 sind für diesen Fall anwendbar.

Vorteile der Ladestations-Anbindung in AF2 Variante a:

1. **Synchronisation der Zugriffe**: Kund_innen greifen, analog zu der Mobilfunk-Anbindung im Anwendungsfall ausschließlich über CPO/CPMS Schnittstellen auf die eigene Ladestation zu. Der CPO kann somit die Anforderungen von Kund_innen und ihm selber synchronisieren, d.h. Kompromisse der möglicherweise in Konflikt befindlichen Anforderungen finden. Dieser Single-Point-Of-Access vereinfacht aus technischer Sicht die Konfliktlösung und Ansteuerung bzw. Priorisierung des Zugriffs.
2. **Unabhängigkeit von Mobilfunk:** Die Steuerung der Ladestation ist für den CPO möglich, wenn vor Ort bei Kund_innen keine Mobilfunk-Anbindung vorhanden ist.
3. **Reduktion von Kosten und Komplexität:** Da Kund_innen für gewöhnlich ein eigenes LAN betreiben, entfallen Logistik, Infrastruktur und Betrieb der Mobilfunk-Anbindung (sowie entsprechende laufende Kosten).
4. **Dedizierte Internet-Anbindung:** Als technische Möglichkeit kann evaluiert werden, ob Internet-Anbieter (ähnlich wie z.B. in der Telekommunikation bei A1overIP Video Streaming) eigene Adressen und eigene QoS-gesicherte Kanäle (z.B. DSL) als Service für CPOs anbieten können. D.h. das CPMS könnte über einen VPN mit dem Internet-Anbieter der Kund_innen kommunizieren. Der Internet-Anbieter kann in der Folge QoS-gesicherte Verbindungen auf Ebene 1 und 2 anbieten (eigenen DSL-Kanal), der im DLS-Modem der Kund_innen auf einem eigenen Ethernet-Port terminiert wird. An diesem Port wird die Ladestation angeschlossen – isoliert vom restlichen Netz der Kund_innen. So eine Anbindung wäre weitgehend abgeschottet vom Internet und dementsprechend sicherer als eine normale Kommunikation zur Steuerung der Ladestation.

Nachteile der Ladestations-Anbindung in AF2 Variante a:

1. **Steuerung der Ladestation erfordert funktionales Kund_innen-Kommunikationsnetz:** Die Internet-Anbindung von Kund_innen wird somit zum Single-Point-of-Failure. Sowohl zu geringe Kapazität, zu hohe Auslastung, als auch (beabsichtigte oder unbeabsichtigte) Konfigurations- oder Hardware-Fehler des Kund_innen-Netzes können die Steuerung der Ladestation durch den CPO erschweren oder im Extremfall verhindern. Das gilt sowohl für drahtgebundene Anbindung (LAN) als auch für Funkverbindung (WLAN).
2. **Eingriffsmöglichkeiten von Kund_innen:** sofern es ihnen Vorteile bringt (und die Ladestation im offline-Betrieb funktional ist), können Kund_innen die Kommunikationsnetz-Anbindung der Ladestation jederzeit unterbrechen. Möglichkeiten reichen vom Abstecken des LAN-Kabels bis zum softwaremäßigen Blockieren der Ladestation auf IP-Ebene in den Zugangsgeräten (z.B. im Kund_innen-eigenen xDSL-Modem oder Router/Switch).
3. **Gefährdung durch lokale Systeme und Malware:** der CPO hat keinerlei Steuerungs-, Monitoring-, oder Kontrollmöglichkeit im LAN der Kund_innen. Kompromittierte Geräte (in Abbildung 22 beispielsweise der rot eingefärbte „CSO PC (infiziert)“) können in heute typischen Konfigurationen von Kund_innen-LANs die Ladestationen über längere Zeiträume überwachen, Schwachstellen aktiv austesten und missbrauchen. Gemäß den in Kapitel 3.4.4 getroffenen Annahmen kann man davon ausgehen, dass ein Angreifer die Ladestation(en) nicht permanent

vom CPO trennen kann. Als Gegenmaßnahme gegen die Gefährdung durch lokale Systeme muss detailliertes Monitoring unverlangter Kommunikation auf der Ladestation erfolgen: die Ladestation muss verdächtige Pakete monitoren und unverzüglich dem CPO melden. Prozesse sollten definiert werden, damit der CPO Kund_innen informieren und entsprechende Behebung beantragen kann.

4. **Notwendigkeit der Isolation der Ladestation im Kund_innen LAN:** Um die Sicherheit der Ladestation zu verbessern (und gleichzeitig die Privatsphäre der Kund_innen zu schützen, siehe den folgenden Punkt) wird dringend empfohlen, die Ladestation vom Rest des Kund_innen LANs mittels eines dedizierten VLANs (siehe Kapitel 1.1 (Punkt 10), 3.1.2 und 3.4.2) zu isolieren. Diese Lösung ist gleichzeitig eine hervorragende Gegenmaßnahme um den vorherigen Punkt (Gefährdung durch lokale Systeme und Malware) zu entschärfen bzw. zu eliminieren. Technische Lösungen gibt es bereits in der Praxis für Echtzeit-Dienste wie z.B. A1overIP Video Streaming, das eine garantierte Bandbreite benötigt um nicht von Datentransfers der Kund_innen gestört zu werden. In diesem Fall bietet das vDSL-Modem einen eigenen Ethernet-Port an, an dem das zu isolierende Gerät angeschlossen wird. Voraussetzung dafür ist jedoch, dass die Hardware der Kund_innen diese Funktionalität unterstützt und korrekt konfiguriert werden kann. Fraglich ist, ob es eine Akzeptanz gibt, dass z.B. CPOs geeignete xDSL-Modems stellen (analog zu Telekom-Betreibern bei IP-basiertem Video). Eine weitere Möglichkeit wäre z.B. ein eigenes, dediziertes WLAN für die Ladestation anzubieten. Herausforderungen bei all diesen Lösungen sind jedoch, dass:
    a. Die notwendige Hardware vorhanden sein muss (DSL/Kabel-Modem oder -Router mit VLAN-Unterstützung) und korrekt konfiguriert wird.
    b. Die Verkabelung vor Ort die Maßnahme unterstützt (dediziertes LAN-Kabel zwischen Modem und Ladestation) bzw. alternativ ein zweites, getrenntes WLAN zulässig ist.
    c. Der Zugriff des CPMS bzw. CPO auf die Ladestation sichergestellt sein muss.
    d. Ladestationen auch andere, systemrelevante Dienste (wie z.B. DNS) nutzen können, aber aus dem Internet ausschließlich für den CPO bzw. dessen CPMS erreichbar sind. Realisierbar wäre so ein Zugang und Schutz z.B. mittels einem dedizierten VPN zwischen CPO und den Modems von Kund_innen.
5. **Gefährdung der Privatsphäre von Kund_innen:** In Abwesenheit der unter Punkt 4 (Isolation der Ladestation) erwähnten Funktionalität kann der CPO eine im Kund_innen (W)LAN befindliche Ladestation, wie bereits in Kapitel 3.4.2 detailliert beschrieben, missbräuchlich als sogenannten Jump-host verwenden. Angemerkt werden muss, dass diese Gefährdung generisch ist und potentiell neben Ladestationen jeden Hersteller und jedes Gerät betrifft (insbesondere SmartHome-Geräte, aber auch Wechselrichter, Wärmepumpen, usw), das mit dem LAN der Kund_innen verbunden ist und gleichzeitig externen Software-Zugriff für die Hersteller der Geräte implementiert. Als Beispiel für potentiell Privatsphäre-gefährdende Software kann z.B. ein Smart-TV mit Konfiguration über Web-Interfaces des Herstellers, aber auch Monitoring- oder Konfigurationstool eines Wechselrichters mittels Web-Interfaces in der Cloud des Herstellers genannt werden.
6. **Angriffsfläche für interne und externe Angriffe (DoS und DDoS, Kapitel 5.4.1.6):** Im Vergleich zu der bei Mobilfunk gut abgeschotteten Kommunikation zwischen Ladestation und CPMS bietet Anwendungsfall 2a eine deutlich größere Angriffsfläche, die aber über Sicherheitsmaßnahmen teilweise beherrscht werden kann. Die Fälle werden im Folgenden im Detail besprochen:
    a. **(D)DoS Angriffe auf die Ladestation aus dem Kund_innen-(W)LAN:** falls keine Isolation der Ladestation mittels VLAN besteht, können von Malware infizierte Geräte der Kund_innen aus dem eigenen (W)LAN die Ladestation angreifen. AF2a hat diesbezüglich den großen Vorteil, dass die Konfiguration und Steuerung der

Ladestation ausschließlich über das CPMS bzw. vom CPO erfolgt. Da andere Geräte im LAN nicht auf die Ladestation zugreifen dürfen/sollen/müssen, kann eine Software-Firewall in der Ladestation Pakete aus dem LAN verwerfen (ausgenommen legitime Kommunikation mit dem Internet-Modem bzw. Pakete vom CPMS). Dennoch ist davon auszugehen, dass bei Infektion mehrerer leistungsfähiger PCs im Kund_innen-LAN ein erfolgreicher DoS-Angriff auf die Ladestation möglich ist.

b. **(D)DoS Angriffe auf die Ladestation aus dem Internet:** Angriffe aus dem Internet sind möglich, aber aufwändig für Angreifer. In Österreich ist es üblich, dass Festnetz- und Mobilfunk-Betreiber den Internet-Modems von Kund_innen dynamische öffentliche (oder sogar private) IPv4 und dynamische öffentliche IPv6-Adressen (Präfixe) zuweisen. Diese Adressen ändern sich alle paar Stunden (typischerweise 8-24 Stunden). Angreifer müssen daher für einen Angriff die aktuelle, öffentliche IP-Adresse des Internet-Modems der Kund_innen kennen. Sofern diese Bedingung erfüllt ist, muss (bei einer genügend großen Anzahl von angreifenden Stellen im Internet) davon ausgegangen werden, dass die Internet-Verbindung von Kund_innen mit einem DDoS Angriff lahmgelegt werden kann. Das Internet-Modem der Kund_innen kann die große Anzahl an einkommenden Paketen nicht mehr handhaben, so dass die Ladestation nicht oder nur mit hoher Verzögerung erreichbar ist. Ein großflächiger Angriff (auf viele Ladestationen gleichzeitig) setzt voraus, dass Angreifer Wege finden, um die aktuellen IP-Adressen all dieser Ladestationen (bzw. die öffentliche Adresse von deren Internet-Modems) zu identifizieren. Es muss deshalb empfohlen werden, die Adress-Information von kontrollierten Ladestationen bestmöglich zu schützen.
c. **ARP Spoofing Angriffe im Kund_innen (W)LAN:** ARP Spoofing ist ein Mechanismus, der im LAN verwendet werden kann, um Geräte zu impersonieren. D.h. Angreifer melden sich statt der Ladestation an und können sich auf diese Weise evtl. als MitM zwischen Modem und Ladestation einschleusen. Aufgrund der Ende-zu-Ende Verschlüsselung mittels TLS und bei Vorhandensein (und Überprüfung) von Zertifikaten sollte im AF2a ARP Spoofing keine Entschlüsselung der Kommunikation erlauben.
d. **(D)DoS Angriffe auf das CPMS durch Ladestationen:** bei Kompromittierung einer großen Anzahl von Ladestationen durch einen Angreifer (z.B. über ein kompromittiertes Firmware-Image) ist davon auszugehen, dass diese die Last am CPMS so erhöhen können, dass das CPMS in Überlast gerät und Kontrolle der Ladestationen nicht mehr zeitgerecht ausgeführt werden kann. Da die Datenkommunikation mit Ladestationen aber deterministische Muster aufweist, sollte ein vorgeschaltetes Monitoring/IDS bzw. eine Firewall auf Seiten des CPO Anomalien erkennen und Gegenmaßnahmen treffen können.
e. **(D)DoS Angriffe auf das CPMS aus dem Internet:** Bei einem Angreifer mit genügend Ressourcen muss davon ausgegangen werden, dass er das CPMS bzw. den gesamten CPO mittels (D)DoS Angriff aus dem Internet lahmlegen kann. Erschwert wird eine Verteidigung des CPO gegen Angriffe aus dem Internet durch die Tatsache, dass Kund_innen-Modems (Kabel, DSL, Mobilfunk) ihre IPv4-Adresse und IPv6-Adressen regelmäßig, dynamisch ändern – und damit auch die Kontaktadresse der Ladestation. D.h. CPOs müssen legitime Verbindungen von Ladestationen von beliebigen IP-Adressen erwarten und annehmen; eine selektive Einschränkung der Firewall-Regeln des CPOs auf erlaubte oder unerwünschte IP-Adressbereiche wird in der Praxis kaum realisierbar sein. Ein Limitieren der Rate aller einkommender Pakete durch den CPO ist eine sehr grobe Lösung, die bei Störungen oder Hochlastfällen im Netz auch negative Auswirkungen haben kann.

7. **Fehlende lokale Steuerungsmöglichkeit durch Kund_innen im Störungsfall:** Bei der Variante AF2a können Kund_innen die Ladestation nicht lokal steuern. D.h. sowohl (i) eine funktionale Internet-Anbindung – genauer: ein funktionaler Pfad zum CPO – als auch (ii) ein funktionales CPMS/Backend sind Voraussetzung für eine Kontrolle der Ladestation durch Kund_innen. Bei Ausfall der eigenen Internet-Anbindung oder Störungen des CPO/CPMS können Kund_innen die Ladestation nicht steuern. Eine Möglichkeit für Zugriff der Kund_innen im Notfall ist der lokale Access-Point, den einige Hersteller auf ihren Ladestationen implementieren. Kund_innen könnten sich mit ihrem Smartphone oder Laptop direkt auf diesen Access Point verbinden und die Ladestation bei Bedarf steuern. Verbunden damit ist der Nachteil, dass Kund_innen dieses Interface auch missbrauchen könnten (Internet-Ausfall vortäuschen um Ladestation direkt zu steuern).

Zusamenfassung Zugriff über Kund_innen (W)LAN (AF2a): Die Anbindung der Ladestation über Kund_innen-LAN mit Steuerungsmöglichkeit der Ladestation ausschließlich über den CPO (Variante 2a) bedingt eine höhere Angriffsfläche gegenüber der Mobilfunk-Anbindung. Einige Angriffsmöglichkeiten, die in Fall 2b angeführt werden, entfallen jedoch. Empfehlenswert ist jedenfalls, sofern technisch machbar, eine Isolation der Ladestation in einem eigenen VLAN (technisch ähnlich wie bei Telekom-Diensten z.B. bei A1overIP Video Streaming realisiert).

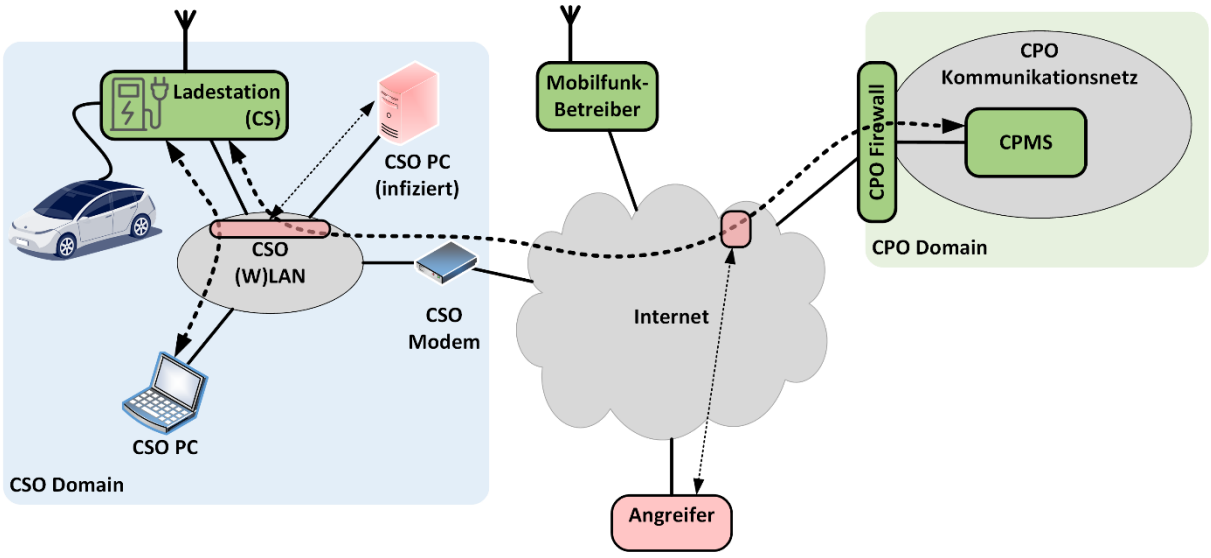

*Abbildung 23: Angriffsmöglichkeiten bei Steuerung der Ladestation durch den CPO über das Kommunikationsnetz der Kund_innen. **Variante b:** Kund_innen haben direkten Zugriff (über WLAN) auf die Ladestation..*

Variante b des Anwendungsfalls 2 entspricht weitgehend der Variante a. Gegenüber Variante a, in der Kund_innen ausschließlich über das CPO-Interface auf die eigene Ladestation zugreifen konnten, haben Kund_innen bei Variante b direkten Zugriff auf ihre Ladestation (dargestellt in Abbildung 23 durch den zusätzlichen Pfeil <CSO PC> zu <Ladestation>). Alle generischen Maßnahmen und Anforderungen gemäß Kapitel 5.4.1 sind für diesen Fall anwendbar.

Gegenüber der in Abbildung 22 dargestellten Variante a bzw. der in der Folge herausgearbeiteten Vorteile und Nachteile fallen einige Änderungen an:

Vorteile der Ladestations-Anbindung in AF2 Variante b:

1. **Synchronisation der Zugriffe:** Der genannte Vorteil entfällt bei Variante b, der vorhandene, parallele Zugriff wird zum Nachteil – **Vorteil-Text der Variante a wird bei Variante b gestrichen.**
2. **Unabhängigkeit von Mobilfunk:** Ident zu Variante a
3. **Reduktion von Kosten und Komplexität:** Ident zu Variante a
4. **Dedizierte Internet-Anbindung:** Ident zu Variante a.
5. **Lokaler Zugriff:** zusätzlich zu Variante a haben Kund_innen die Möglichkeit, ihre Ladestation auch bei fehlendem Internet-Zugriff oder nicht verfügbarem CPO zu steuern. Kund_innen haben die (theoretische) Möglichkeit, im Störungsfall oder bei Angriffen auf Anweisung des CPO geeignete manuelle Konfigurationen der Ladestation vorzunehmen.

Nachteile der Ladestations-Anbindung in AF2 Variante b:

1. **Steuerung der Ladestation durch CPO erfordert funktionales Kund_innen-Kommunikationsnetz:** Ident zu Variante a.
2. **Eingriffsmöglichkeiten von Kund_innen:** Text von Variante a trifft zu. Ergänzend haben Kund_innen durch die eigene Steuerungsmöglichkeit Wege, Ladeprofile des CPO ggf. zu umgehen (d.h. ggf. explizites Interesse an einer nicht-funktionalen CPO-Anbindung).
3. **Gefährdung durch lokale Systeme und Malware:** Ident zu Variante a. Zusätzlich noch direkter Steuerungszugriff aus Kund_innen-LAN mit zusätzlicher Angriffsfläche aufgrund der Exposition der Ladestation gegenüber lokalen, kompromittierten Systemen der Kund_in.
4. **Notwendigkeit der Isolation der Ladestation im Kund_innen LAN:** Ident zu Variante a. Zusätzliche Herausforderung bzw. Erweiterung der Angriffsfläche bei Isolation der Ladestation in einem eigenen VLAN ist der notwendige, steuernde Zugriff durch (in einem anderen VLAN befindlichen) Kund_innen-PCs.
5. **Gefährdung der Privatsphäre von Kund_innen:** Ident zu Variante a. Zusätzlich noch berücksichtigt werden muss (bei Vorsehen expliziter Trennung durch VLANs), dass ein Zugriff durch Kund_innen auf die Ladestation keinen Zugriff der Ladestation auf das Kund_innen-VLAN ermöglichen darf.
6. **Angriffsfläche für interne und externe Angriffe (DoS und DDoS, Kapitel 5.4.1.6):** Die Angriffsfläche wird bei Variante b durch den direkten Kund_innen-Zugriff auf die Steuerung der Ladestation etwas erhöht:
    a. **(D)DoS Angriffe auf die Ladestation aus dem Kund_innen-(W)LAN:** sind grundsätzlich möglich und gefährden die Ladestation. Eine Abschottung der Ladestation gegenüber DDoS Angriffen aus dem Kund_innen-LAN ist ohne oder mit dediziertem VLAN fordernd und setzt Einschränkungen voraus (z.B. steuernden Ladestations-Zugriff nur von ausgewählten Kund_innen-IP-Adressen). Bei Infektion mehrerer leistungsfähiger PCs im Kund_innen-LAN ist ein erfolgreicher DoS-Angriff auf die Ladestation möglich und kaum zu verhindern.
    b. **(D)DoS Angriffe auf die Ladestation aus dem Internet:** ident zu Variante a.
    c. **ARP Spoofing Angriffe im Kund_innen (W)LAN:** ident zu Variante a.
    d. **(D)DoS Angriffe auf das CPMS durch Ladestationen:** ident zu Variante a.
    e. **(D)DoS Angriffe auf das CPMS aus dem Internet:** ident zu Variante a.
7. **Fehlende lokale Steuerungsmöglichkeit durch Kund_innen im Störungsfall:** entfällt, da Kund_innen sehr wohl lokal steuern können.
8. **Synchronisation der Steuerungsmöglichkeiten:** Zusätzlich zu Variante a muss bei Variante b die Steuerung der Ladestation durch den CPO bzw. durch Kund_innen synchronisiert werden.

Zusammenfassung Zugriff über Kund_innen (W)LAN (AF2b): Die Anbindung der Ladestation über Kund_innen-LAN mit Steuerungsmöglichkeit der Ladestation über CPO oder lokal durch Kund_innen

(Variante 2b) erhöht die Angriffsfläche gegenüber AF2a. Eine Isolation der Ladestation in einem eigenen VLAN (technisch ähnlich wie bei Telekom-Diensten z.B. bei A1overIP Video Streaming realisiert) ist schwierig, da der direkte Zugriff von Kund_innen (als wichtigstes Merkmal von AF2b) damit kompliziert wird. Die Studienautor_innen bevorzugen aus Sicherheitssicht AF2a gegenüber AF2b: die Vorteile direkter Steuerung durch Kund_innen bei AF2b wiegen die Nachteile in Bezug auf Sicherheit gegenüber AF2a aus Sicht der Studienautor_innen nicht auf.

5.4.4 AF3: Ladestations-Zugriff über das Kommunikationsnetz der Kund_innen und über Mobilfunk

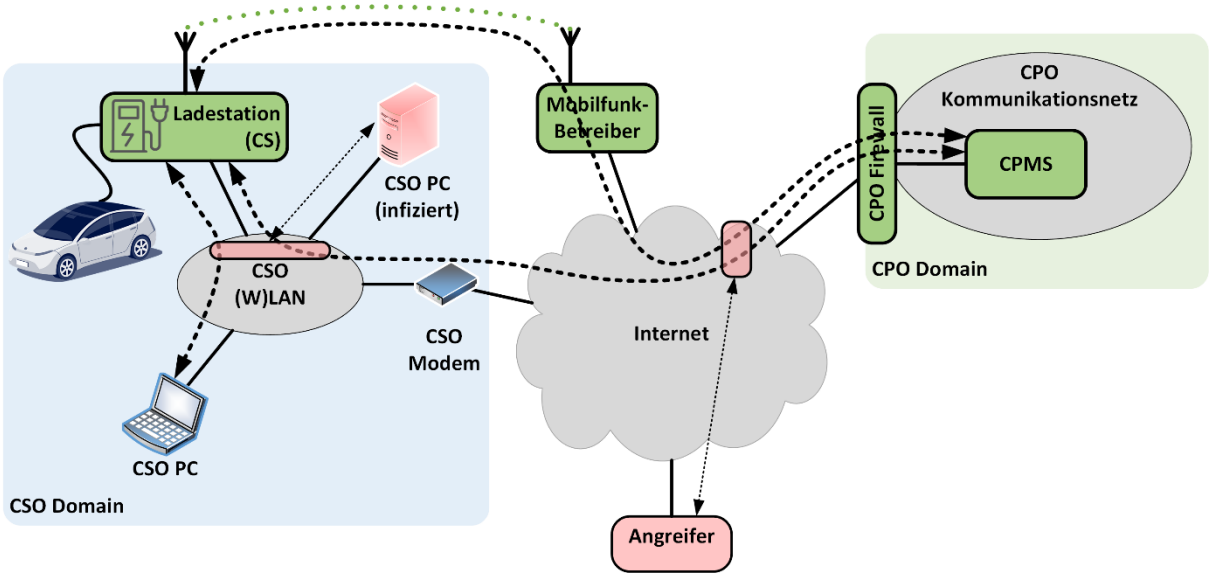

Abbildung 24: Angriffsmöglichkeiten bei Steuerung der Ladestation durch den CPO sowohl über Mobilfunk als auch über das Kommunikationsnetz der Kund_innen. Kund_innen haben zusätzlich direkten Zugriff (über WLAN) auf die Ladestation.

Der Anwendungsfall AF3 – Steuerung der Ladestation durch den CPO sowohl über Mobilfunk als auch über Kund_innen LAN – bietet aus CPO-Sicht und Kund_innensicht den **Vorteil größtmöglicher Redundanz**. Ansonsten gibt es hauptsächlich Nachteile, sowohl für CPO als auch für Kund_innen.

Vorteile der Ladestations-Anbindung in AF3:

1. **Redundante Steuerungspfade:** sobald ein Kommunikationsnetz ausfällt, kann auf das andere zurückgegriffen werden.

Nachteile der Ladestations-Anbindung in AF3:

1. **Aggregierte Nachteile von AF1 und AF2b.**
2. **Zusätzliche Gefährdung der Privatsphäre von Kund_innen:** Durch Anbindung der Ladestation über Mobilfunk und Kund_innen-(W)LAN hat der CPO potentiell redundante Möglichkeiten um Kund_innen auszuspähen.

Zusammenfassung Zugriff über Mobilfunk und über Kund_innen (W)LAN (AF3): Die Anbindung der Ladestation sowohl über Mobilfunk als auch über Kund_innen-(W)LAN mit Steuerungsmöglichkeit der Ladestation über CPO oder lokal durch Kund_innen bietet deutlich bessere Redundanz: falls eine Anbindung ausfällt, kann der CPO auf den anderen Kommunikationspfad zurückgreifen. Dem gegenüber stehen die aggregierten Nachteile von AF1 und von AF2: Kosten für den CPO, erhöhte Angriffsfläche für CPO und Ladestation und potentielle Gefährdung der Privatsphäre von Kund_innen durch den CPO. Die nicht vorhandene Möglichkeit der Kontrolle der CPO-Mobilfunkanbindung der

Ladestation durch Kund_innen schafft potentielle Pfade für den CPO zum Abgriff von Kund_innen-Daten.

5.5 Angriffsszenarien und Verteidigungsmaßnahmen

In den Kapitel 3 beschriebenen Szenarien wurde davon ausgegangen, dass sich der Angreifer außerhalb des Kund_innen LAN befindet und alle Arten von Angriffen über das Internet ausführt. Der folgende Abschnitt geht detailliert auf gängige Angriffsszenarien ein, die in dieser Konstellation auftreten können. Außerdem gibt er Beispiele für Abläufe von Angriffen, wenn sich der Angreifer innerhalb des Netzes des Benutzers befindet.

Erste Herausforderung für Angreifer ist die Kommunikation mit Geräten innerhalb des Kund_innen-LAN, wenn dieses LAN durch eine Firewall oder Network Address Translation (NAT) abgeschottet wird. Typischerweise wäre der Einstiegspunkt des Angreifers der Internet-Router des Benutzers, der alle eingehenden Anfragen von externen Quellen blockieren sollte. Angreifer können diese Beschränkung durch verschiedene Techniken umgehen, z. B. durch Hole Punching, bei dem der Angreifer bereits offene Transportports nutzt. Eine andere Methode ist die Installation kompromittierter Firmware auf einem der mit dem Netzwerk verbundenen Geräte der Kund_innen, die es dem Angreifer ermöglicht, über dieses Gerät eine Verbindung mit dem externen Netzwerk zu initiieren. Die kompromittierte Firmware kann durch eine Vielzahl von Methoden hochgeladen werden, z. B. durch physische Manipulation (unter Verwendung von Hardware-Backdoors), Fälschung der Herstelleridentität usw.

Sobald die anfängliche Herausforderung der Umgehung von Firewalls und NAT überwunden ist, wird eine breite Palette von Angriffen möglich. In dieser Studie betrachten wir zwei Hauptszenarien: (1) die Ladestation wird kompromittiert und anschließend missbraucht oder zur Ausführung von Proxy-Angriffen verwendet, oder (2) ein anderes Gerät innerhalb des Kund_innen LAN wird kompromittiert und zum Angriff auf die Ladestation verwendet. Diese Szenarien verdeutlichen die Bedeutung umfassender Sicherheitsmaßnahmen, um sich gegen ein breites Spektrum potenzieller Angriffe zu schützen, sowie die Notwendigkeit einer ständigen Überwachung und Wartung aller mit dem LAN verbundenen Geräte.

5.5.1 Kompromittierte Ladestation

Bei einer erfolgreichen Kompromittierung wird davon ausgegangen, dass der Angreifer die vollständige Kontrolle über die Ladestation erlangt hat und diese für zwei Hauptzwecke nutzen kann: direkte Kontrolle und Datendiebstahl oder Verwendung als Proxy, d.h. als Schnittstelle, für die Ausführung von Angriffen. Nachfolgend sind Beispiele für mögliche Angriffe angeführt, die auftreten können:

- **Denial of Service (DoS)**: Der Angreifer kann die Ladestation als Sprungstelle (sogenannten Jump-Host) oder als Urheber des Angriffs verwenden, wobei zu beachten ist, dass Ladestationen in der Regel nicht über die erforderliche Rechenleistung zur Ausführung solcher Angriffe verfügen. Das Ziel des DoS-Angriffs kann entweder außerhalb des lokalen Netzes liegen, z. B. ein Webserver, oder innerhalb des Netzes, z. B. ein anderes anfälliges Gerät. In beiden Fällen scheint der Angriff von der Ladestation auszugehen. Es ist wichtig zu beachten, dass dies nur möglich ist, wenn die Ladestation mit dem lokalen Netz verbunden ist. Ladestationen, die über Mobilfunkverbindungen angeschlossen sind, werden in der Regel von den Providern in einem Subnetz isoliert. Jeder von der Ladestation ausgehende Datenverkehr müsste die Firewalls des Providers umgehen, was bei den derzeitigen Infrastrukturen unterbunden werden sollte, da die zulässigen Dienste streng begrenzt sind. Allerdings können solche Angriffe immer noch auf zugelassene Diensteanbieter wie NTP- oder DNS-Server

abzielen. Diese Einschränkung gilt für alle folgenden Angriffe, wenn die Ladestation nur über Mobilfunk verbunden ist.

- **Brute Forcing**: Ähnlich wie beim vorigen Angriff können kompromittierte Ladestationen als Sprungstelle oder als Quelle von Brute-Force-Angriffen verwendet werden, z. B. für den Versuch, Zugang zu anderen externen oder internen Geräten zu erhalten. Der Angreifer nutzt die Ressourcen der Ladestationen direkt oder als Proxy um Brute-Force Angriffe durchzuführen. Die gleichen Schlussfolgerungen über weitere Möglichkeiten gelten auch hier.
- **Verzögerung und passives Monitoring**: Ist die Ladestation mit einem CPMS verbunden, kann der Angreifer Verzögerungsangriffe (sogenannte Time-Delay Attacks) durchführen, um den Empfang von wichtigen Kontrollmeldungen oder Firmware-Updates zu verzögern oder zu verhindern. Durch Lauschangriffe kann der Angreifer persönliche und private Daten wie geheime Kennungen und das Ladeverhalten ausspähen und so weitere Erkenntnisse über Kund_innen und das CPMS gewinnen. Diese Angriffe können durch die Verwendung von Hintertüren in der kompromittierten Firmware durchgeführt werden, um wichtige Daten zu exfiltrieren, oder durch die Implementierung von Änderungen am Kommunikationsprotokoll, um Verzögerungen einzuführen oder Antworten zu verhindern.
- **Man-in-the-Middle (MitM)**: In diesem Szenario ist ein herkömmlicher MitM-Angriff nicht möglich, da der Angreifer den zwischen der Ladestation und dem CPMS ausgetauschten Verkehr nicht abfangen kann. Allerdings kann der Angreifer MitM auf der Softwareebene in der Firmware (d. h. nicht auf der Verbindung) implementieren, wodurch er Kontrollnachrichten aus der Ferne manipulieren kann. Da der Angreifer direkten Zugriff auf die Ladestation hat, spielt es keine Rolle, ob die Verbindung zum CPMS verschlüsselt ist oder nicht, und TLS wäre in diesem Fall wahrscheinlich nicht wirksam, da die Kommunikation am End-Host unverschlüsselt ist.
- **Manipulationen des Ladeprofils**: Diese Art des Angriffs wirkt sich direkt auf die Ladestation aus, kann leicht mit Hilfe einer bösartigen Firmware ausgeführt werden und soll eher dem Nutzer als anderen Geräten schaden.

Die Analyse möglicher Angriffe zeigt, dass ein Großteil davon durch das Einschleusen kompromittierter Firmware in die Ladestation ermöglicht wird. Im Falle einer nicht kompromittierten Firmware sind viele dieser Angriffe nicht durchführbar. Es ist jedoch auch möglich, dass ein Angreifer andere Geräte im LAN der Kund_innen kompromittiert, wie in den folgenden Abschnitten beschrieben.

5.5.2 Kompromittierte angeschlossene Geräte

Die Kompromittierung eines Geräts oder Systems im Kund_innen LAN ermöglicht eine Vielzahl von Angriffen mit potenziell negativen Auswirkungen auf Kund_innen. Dieser Abschnitt konzentriert sich auf Angriffe, bei denen das kompromittierte Gerät auf die Ladestation von Kund_innen abzielt. Im Folgenden finden sich Beispiele für mögliche Angriffe:

- **DoS**: In diesem Szenario zielt das böswillige Gerät mit einem DoS-Angriff auf die Ladestation ab, mit dem Ziel, sie für Kund_innen oder den CPO nicht mehr verfügbar zu machen. Dies wird erreicht, indem zunächst ein Gerät kompromittiert wird und der Angriff innerhalb des LAN ausgeführt wird. Dabei wird davon ausgegangen, dass die Ladestation mit dem LAN verbunden ist und mindestens einen offenen Port auf Transportebene (z.B. TCP oder UDP) hat.
- **Brute-Forcing**: Dieses Szenario ähnelt dem zuvor beschriebenen Brute-Forcing, mit dem einzigen Unterschied, dass das Ziel die Ladestation ist. Ein Angreifer kann ein kompromittiertes Gerät verwenden, um die Anmeldeinformationen der Webschnittstelle einer Ladestation zu erzwingen. Ein erfolgreicher Angriff würde dem Angreifer Zugriff auf eine Reihe von Steuerungsoptionen gewähren, was ihm weitere Angriffe und Fehlkonfigurationen ermöglicht.

Ein eher unwahrscheinliches Szenario ist, dass ein Angreifer die Kontrolle über ein angeschlossenes Gerät erlangt und eine Kommunikation mit der Ladestation einleitet, während er sich als CPMS ausgibt. Dies ist nur möglich, wenn keine Zertifikate implementiert sind, was den Mindestanforderungen für OCPP Security Profile 3 oder 2 in Kapitel 5.4.1 widerspricht. Sollte es jedoch zu einem solchen Angriff kommen, so würde dies die Angriffsfläche erheblich vergrößern, da der Angreifer die vollständige Kontrolle über die Ladeprofile ausüben und möglicherweise kompromittierte Firmware einschleusen könnte.

Wenn die Ladestation nicht kompromittiert ist, sind aufgrund der TLS-Verschlüsselung und Authentifizierung verschiedene Formen von Angriffen, die eine Manipulation oder ein Abhören des Verkehrs von oder zu der Ladestation beinhalten, sehr unwahrscheinlich, wenn nicht sogar unmöglich. Daher sind Angriffe in diesem Szenario, sofern sie nicht mit anderen Techniken kombiniert werden, im Allgemeinen weniger schädlich als solche, bei denen die Ladestation kompromittiert wurde.

Bei allen oben beschriebenen Szenarien wird davon ausgegangen, dass sich der Angreifer außerhalb des Kund_innen LAN befindet und unter Umgehung der Firewalls agiert. Das schwerwiegendste Szenario ist, wenn die Ladestation direkt mit dem Kund_innen-LAN und darüber hinaus mit dem Internet verbunden ist. Für den Anwendungsfall AF1 (Anbindung Ladestation ausschließlich über Mobilfunk) ist aufgrund der fehlenden Anbindung der Ladestation zum Kund_innen LAN selbst bei kompromittierten Geräten im Kund_innen-LAN von keiner Gefährdung der Ladestation auszugehen. Weiters sieht die Anbindung der Ladestation durch den CPO mittels Mobilfunks eine weitgehende Isolation der Ladestationen untereinander und gegenüber dem Internet vor. Ausgehender Datenverkehr der Ladestationen über die CPO-Infrastruktur sollte in diesem Fall durch den CPO beobachtet oder unterbunden werden, und im Anlassfall Alarme auszulösen.

5.5.3 Verteidigungsmechanismen

Einige generische Vorsichtsmaßnahmen verringern sowohl die Angriffsfläche selbst als auch die Wahrscheinlichkeit, dass ein Angreifer die vorherigen Angriffe ausführt:

- **Geräteisolierung**: Die Ladestation kann mithilfe von VLANs oder speziellen Zugangspunkten mit Firewalls vom Kund_innen LAN isoliert werden. Dies ermöglicht die Trennung von Geräten innerhalb desselben LAN und verhindert Angriffe in beide Richtungen, d. h. von der Ladestation aus, um andere lokale oder externe Geräte anzugreifen, und von anderen Geräten aus, um die Ladestation anzugreifen. Wir empfehlen dringend die Implementierung dieses Konzepts um Probleme zu umgehen, die mit dem Anschluss der Ladestation in LANs mit anderen, ungesicherten Geräten verknüpft sind.
- **Trennung der Verbindung**: Die einfachste Möglichkeit, eine Ladestation zu schützen, besteht darin, jegliche Kommunikation zu unterbinden. Dies ist jedoch nicht immer möglich, insbesondere in Fällen, in denen der CPO dies aus verschiedenen Gründen nicht zulässt, z. B. aus Gründen der Abrechnung oder der Vertragsleistungen.
- **Regelmäßige Aktualisierungen**: Der beste Weg, um sicherzustellen, dass keine (oder nur wenige) Sicherheitslücken vorhanden sind, besteht darin, die Ladestation und alle angeschlossenen Geräte auf dem neuesten Stand zu halten. So können die neuesten Patches und Fehlerbehebungen installiert werden, was die Sicherheit erhöht.
- **Beobachtung des Datenverkehrs**: Technisch erfahrene Kund_innen können Software für Kommunikationsmonitoring im Kund_innen-LAN installieren, um verdächtige Aktivitäten zu identifizieren – z.B. ob einige Geräte in ggf. böswilliger Absicht unüblichen Datenverkehr verursachen oder Verbindungen zu unbekannten Hosts herstellen. Dies kann ein guter Indikator für einen laufenden Angriff sein.

- **Installation von Firewalls**: Eine weitere wirksame Lösung ist die Installation von Firewalls und deren entsprechende Konfiguration im lokalen Netz. Die meisten modernen Router bieten Basis-Firewalls, die für den einfachen Gebrauch ausreichen sollten, aber sie können auch erweitert werden, um den Verbindungsaufbau von intelligenten Geräten zu begrenzen, insbesondere im Falle einer Ladestation.
- **Aktive Suche nach Schwachstellen**: CPOs und Hersteller können einerseits mit der Beauftragung externer Experten für Penetration Tests versuchen, potentielle Schwachstellen der Ladestationen und Systeme zu identifizieren. Gleichzeitig kann man über sogenannte Bounty hunt Programme und Belohnungen Anreize für Kund_innen und Unbeteiligte Experten schaffen, um gefundene Schwachstellen zuerst den Herstellern und CPOs zu melden.

6 Zusammenfassung und Schlussfolgerung

Die Erkenntnisse und Messergebnisse der vorherigen Kapitel werden in diesem Kapitel zusammengefasst. Vor- und Nachteile der analysierten Anwendungsfälle werden verglichen und die wesentlichen Anforderungen als Schlussfolgerung der Studie festgehalten.

6.1 Grundlegende Feststellungen und Anforderungen

Wesentliche Schlussfolgerung dieser Studie ist, dass CPOs mit Unterstützung von OCPP eine sichere Steuerung von Ladestationen bei Kund_innen implementieren können, die die Privatsphäre von Kund_innen weitgehend bewahrt. **Generische Voraussetzungen** dafür sind:

1. **Verwendung der JSON/WebSocket-Variante von OCPP** (OCPP-J 1.6 mit Security Extensions gemäß OCPP Whitepaper oder OCPP-J 2.0.1). Die Verwendung der XML/SOAP Variante von OCPP 1.6 (OCPP-S 1.6) hat signifikante Defizite in Bezug auf Sicherheit, Architektur und Kommunikation – unter anderem sieht der OCPP-Standard keine Sicherheitsarchitektur für OCPP-S vor. Aus diesen Gründen soll OCPP-S für eine Steuerung von Ladestationen bei Kund_innen durch den CPO nicht verwendet werden.
2. **Ausschließliche Verwendung von OCPP Security Profile 3 (TLS mit Server- und Client-seitigem Zertifikat) oder OCPP Security Profile 2 (TLS mit serverseitigem Zertifikat)** für die Kommunikation Ladestation-CPMS**.** Die Verwendung von TLS zur Ende-zu-Ende Absicherung ist in allen Fällen unbedingt notwendig! Die Absicherung über Verwendung sogenannter „sicherer“ oder „vertrauenswürdiger“ Netze ist wegen den bekannten Angriffen wie z.B. Downgrade-Angriff bei Mobilfunk kein Ersatz für die Absicherung mittels TLS (evtl. als zusätzliche Sicherungsmaßnahme möglich und empfohlen). Empfohlen wird das Security Profile 3. Verwendbar ist mit einer aus Sicherheitsperspektive akzeptablen Vergrößerung der Angriffsfläche beim CPO auch OCPP Security Profile 2 (nur Server Zertifikat) sofern Randbedingungen erfüllt sind. Insbesondere muss für die sichere Inbetriebnahme der Ladestation:
    a. der Hersteller der Ladestation bei der Produktion einen eindeutigen Schlüssel zur Authentifizierung auf der Ladestation gespeichert haben
    b. der Schlüssel ausschließlich dem CPO/CPMS bekannt und Angreifern weder bekannt, noch von diesen erratbar, noch über andere Kanäle in Erfahrung zu bringen sein, sowie
    c. die Ladestationen eine zuverlässige TLS-Verbindung zum CPMS aufbauen können mit Möglichkeit der Ladestation, den CPMS über Server-Zertifikate zu authentifizieren. In diesem Fall können Angreifer zwar gültige TLS-Verbindungen zum CPMS aufbauen, was die Angriffsfläche des CPMS z.B. bei (D)DoS-Angriffe durch Botnetze deutlich erhöht. Angreifer können sich jedoch auf Applikationsebene **nicht** beim CPMS als

gültige Ladestation authentifizieren, aber eine höhere Last erzeugen. OCPP Security Profile 3, mit Client-Zertifikaten, ist zu bevorzugen, da es die Angriffsfläche verringert und als integrierter Teil von TLS bereits komplexen Security Audits unterzogen wurde.

3. **Gültige Uhrzeit und gültige Zertifikate auf der Ladestation:** Die Zertifikate sind die Basis für TLS-gesicherte Kommunikation zwischen Ladestation und CPMS, haben aber aus Sicherheitsgründen eingeschränkte Gültigkeitsdauer. Für eine sichere Inbetriebnahme der Ladestation (insbesondere die erste Konfiguration) muss sichergestellt sein, dass
    a. Die Uhr der Ladestation bei deren ersten Inbetriebnahme „ausreichend“ genau synchronisiert ist (d.h. in der Größenordnung von Stunden oder Tagen). Dafür gibt es bei Verwendung handelsüblicher batteriegepufferter Uhren und Lagerzeiten von einigen Jahren keine technischen Hindernisse.
    b. Die auf der Ladestation gespeicherten Zertifikate zum Zeitpunkt der Inbetriebnahme der Ladestation gültig sind. Die gespeicherten Intermediate und Root-Zertifikate (bzw. ggf. Client-Zertifikate) der Ladestation müssen so lange gültig sein, dass eine Inbetriebnahme der Ladestation innerhalb des Zeitraums erfolgen kann.
    c. Die verwendeten Zertifikate bei der Inbetriebnahme der Ladestation (genauer: im Zeitraum zwischen Herstellung und Inbetriebnahme) nicht zurückgerufen (revoked) bzw. kompromittiert wurden. Falls eine Kompromittierung stattgefunden hat, kann die Ladestation bei der ersten Inbetriebnahme die gültigen Widerrufslisten (revocation lists) für Zertifikate nicht (sicher) abrufen und Angreifer können sich unter Missbrauch der kompromittierten Zertifikate als MitM einschleusen.
4. **(Vor)Konfiguration durch Hersteller:** Um die sichere ZeroConf Inbetriebnahme von Ladestationen zu ermöglichen (Einschalten an einem Kund_innen LAN mit DHCP IPv4 Adressvergabe und sicherer Kontakt zum CPMS mit anschließender Konfiguration) muss der Ladestations-Hersteller (oder CPO) die Ladestationen von Kund_innen entsprechend vorkonfigurieren. Mindestens eingespeichert werden müssen:
    a. IP-Adresse bzw. Hostname des CPMS
    b. Root und Intermediate-Zertifikate für Prüfung der TLS-Verbindung der Ladestation zum CPMS
    c. Ladestations-Client-Zertifikate (bei OCPP Security Profile 3) oder eindeutiger, dem Angreifer unbekannter und von ihm nicht erratbarer/berechenbarer Schlüssel für Ladestations-Authentifizierung beim CPMS.

6.2 Bewertung Anwendungsfälle

Die Analyse der Vor- und Nachteile der Anwendungsfälle AF0 bis AF3 in Kapitel 5.4 lässt unter Berücksichtigung der Metriken Vertraulichkeit, Integrität, Verfügbarkeit, bzw. Privatsphäre von Kund_innen den Schluss zu, dass **zwei Anwendungsfälle für den praktischen Einsatz empfehlenswert sind.**

1. **AF1 (Steuernder Ladestations-Zugriff des CPO über Mobilfunk ohne lokale Vernetzung der Ladestation, detaillierte Beschreibung in Kapitel 5.4.2).** In der realistischen Annahme von privatem APN, privaten IP-Adressen und intra-APN-Sicherheitsvorkehrungen beinhalten die wesentlichen zusammengefassten Vorteile und Nachteile:
    a) (+) Weitgehende Abschottung vom Internet: jede Ladestation erhält eine feste, private (oder öffentliche) IP-Adresse und ist aus dem öffentlichen Internet nicht erreichbar. Intra-APN-Sicherheit verhindert weiters, dass kompromittierte Ladestationen auf andere Ladestationen oder Geräte zugreifen: nur legitime Gegenstellen (z.B. CPMS, DNS) sind

zugelassen. Aus CPO-Sicht hat das CPMS keine Steuerungs-Schnittstelle im öffentlichen Internet.

b) **(+) Absicherung gegenüber Angriffen und Zugriffen aus Kund_innen-(W)LANs:** da die Ladestation nicht im (W)LAN von Kund_innen angeschlossen ist, können potentielle kompromittierte Geräte im Kund_innen (W)LAN nicht auf die Ladestation zugreifen und sie nicht angreifen.
c) **(+) Wahrung der Privatsphäre von Kund_innen:** Da die Ladestation nicht im (W)LAN von Kund_innen angeschlossen ist, entfällt die Möglichkeit des Auskundschaftens des (W)LANs durch den CPO. Der CPO kann ausschließlich den Gebrauch der Ladestation beobachten.
d) **(+) Synchronisation der Zugriffe von CPO und Kund_innen:** Da Kund_innen ausschließlich über Interfaces des CPO und das CPMS auf ihre Ladestation zugreifen können, kann das CPMS die Zugriffe und Präferenzen von CPO bzw. Kund_innen bzgl. Ladeleistung und Ladeprofile gut synchronisieren und in Einklang bringen.
e) **(-) Folgekosten und Komplexität:** Der Betrieb einer großen Anzahl von SIM-Karten ist für den CPO mit Kosten und Aufwand verbunden.
f) **(-) Abhängigkeit vom Mobilfunk-Betreiber:** Die Steuerung der Ladestation benötigt ein operationales, verlässliches Mobilfunknetz – einschließlich korrekter Konfiguration durch den Mobilfunk-Betreiber (besonders bezüglich privatem APN und Intra-APN-Sicherheit).
g) **(-) Mögliche Downgrade-Angriffe:** Angreifer können bei Anwesenheit vor Ort das Downgrade von 3G und 4G Verbindungen auf 2G Technologie erzwingen und somit die Verschlüsselung auf Mobilfunkebene aufbrechen. Betroffen sind aber ausschließlich Protokolle, die NICHT Ende-zu-Ende TLS verschlüsselt werden, z.B. DNS oder NTP. OCPP im Security-Profil 2 und 3 ist davon nicht betroffen. Details werden in Kapitel 5.4.2 erklärt.
h) **(-) Schwierigkeiten und Folgekosten bei schlechter Funkversorgung:** Bei schlechter Funkversorgung z.B. in Tiefgaragen oder in ländlicher Umgebung kann die Signalqualität für Datenübertragung nicht ausreichen. In diesem Fall sind Lösungen wie Mobilfunk-Repeater des Mobilfunk-Betreibers, dedizierte Leitungen oder eigene Funknetze gemäß Kapitel 5.4.2 notwendig.
i) **(-) Fehlender direkter Zugriff durch Kund_innen und Missbrauch von Steuersignalen:** die Notwendigkeit sofortiger Abschaltung im Notfall (bei Überlast) wird durch Mobilfunk und die entsprechenden Verzögerungen nicht gewährleistet. Als „Not-Aus“ sollten daher andere, redundante Lösungen überlegt werden. Eine Option wäre z.B. die Verwendung von Steuersignalen ähnlich dem „Nachtstrom“ in Stromnetzen. Diese Steuersignale sind jedoch zur Zeit nicht gesichert und können daher theoretisch von Angreifern missbraucht werden.

2. **AF2 Variante a (Steuernder Ladestations-Zugriff des CPO über Kund_innen-Kommunikationsnetz OHNE direkten Kund_innenzugriff auf Ladestation, detaillierte Beschreibung in Kapitel 5.4.3) – unter der Voraussetzung, dass die Ladestation mittels VLAN im Kund_innen-Kommunikationsnetz abgetrennt wird.** Voraussetzung dieser Lösung ist die Annahme, dass das Internet-Modem der Kund_innen einen eigenen, dedizierten Ethernet-Port in einem separaten VLAN (oder ein eigenes WLAN) für die Anbindung der Ladestation vorsieht.
   a) **(+) Möglichkeit der Einschränkung von Internet-Zugriffen auf die Ladestation:** Die Kund_innen-Firewall kann bei Vorhandensein einer bekannten, fixen IP-Adresse des CPMS externe Zugriffe auf das VLAN der Ladestation oder deren IP-Adresse ausschließlich auf die IP-Adresse des/der CPMS einschränken. Damit können Angreifer die Ladestation nicht direkt erreichen (ausgenommen über DoS-Angriffe, die gefälschte Source-IP-Adressen des CPMS verwenden).

b) **(+) Absicherung gegenüber Angriffen und Zugriffen aus Kund_innen-(W)LANs:** da die Ladestation in einem eigenen Kund_innen VLAN hängt, können potentiell kompromittierte Geräte im Kund_innen (W)LAN nicht auf die Ladestation zugreifen und sie nicht angreifen.
c) **(+) Wahrung der Privatsphäre von Kund_innen:** die Ladestation hängt in einem eigenen VLAN. Der CPO kann selbst bei absichtlicher Verwendung der Ladestation als Jump-Host keine im Kund_innen (W)LAN angeschlossenen Geräte sehen oder auskundschaften. Die Privatsphäre der Kund_innen ist demzufolge gegenüber dem CPO weitgehend geschützt. Selbstverständlich ist der CPO über die Nutzung und Ladevorgänge der Ladestation vollständig informiert – das lässt sich bei einer Steuerung der Ladestation nicht vermeiden.
d) **(+) Synchronisation der Zugriffe von CPO und Kund_innen:** Da Kund_innen ausschließlich über Interfaces des CPO und das CPMS auf ihre Ladestation zugreifen können, kann das CPMS die Zugriffe und Präferenzen von CPO bzw. Kund_innen bzgl. Ladeleistung und Ladeprofile gut synchronisieren und in Einklang bringen.
e) **(+) Kostenersparnis:** Gegenüber der Anbindung über Mobilfunk entfallen die laufenden Kosten für SIM-Karten und deren Betrieb.
f) **(-) Abhängigkeit von Kund_innen Internet-Anbindung:** Die Steuerung der Ladestation benötigt ein operationales, verlässliches Kommunikationsnetz und eine permanente Internet-Anbindung von Kund_innen. Die Qualität der Internet-Anbindung von Kund_innen muss den Anforderungen des CPO in Bezug auf Durchsatz, Verfügbarkeit und Verzögerung entsprechen.
g) **(-) Technische Voraussetzungen und Konfiguration der Kund_innen-Internet-Anbindung:** Für die Abtrennung der Ladestation in einem eigenen VLAN (eigener Ethernet-Port) oder einem eigenen WLAN ist entsprechende Hardware-Unterstützung im Internet-Modem notwendig. Technische Expertise mit ähnlichen Lösungen gab es z.B. beim mittlerweile aufgelassenen A1 over IP Video Streaming. Eine Absicherung der Kund_innen-Internet-Anbindung gegen Angriffe aus dem Internet (z.B. Einschränkung des Internet-Zugriffs auf Ladestation auf IP-Pakete mit Absenderadresse CPMS) bedarf technischer Kenntnisse. Technisch machbar wäre auch ein zusätzlich geschützter VPN zwischen Internet-Modem und CPMS oder zwischen Internet-Modem und Internet-Provider mit einem weiteren VPN zwischen Internet-Provider und CPMS.
h) **(-) Herausforderungen beim Schutz des CPO/CPMS:** Die Internet-Anbindung kann unterschiedlichste Internet-Provider, technische Lösungen (VDSL, Kabel, Mobilfunk) und Implementierungsvarianten umfassen. Typisch ist bei Internet-Providern die regelmäßige Änderung der zugewiesenen IPv4-Adresse bzw. des IPv6-Präfixes des Internet-Modems (alle 8-24 Stunden) und somit aller damit angebundener Geräte. Die Firewall des CPO bzw. der CPMS muss also IP- und TLS-Verbindungen von (nahezu) beliebigen IP-Adressen akzeptieren. Eine Einschränkung auf IP-Subnetze oder einzelne Adressen scheint sehr fordernd. Evtl. möglich ist eine (sehr fehleranfällige) Einschränkung auf IP-Adressen, die geographisch Österreich zuordenbar sind (funktioniert z.B. bei StarLink und Sat-Internet nicht). Diese Tatsache öffnet eine große Angriffsfläche für potentielle Angreifer, speziell bei (D)DoS Angriffen, um im Anlassfall den CPMS zu überlasten und somit die Steuerung von Ladestationen zu verunmöglichen. Als mögliche technische Gegenmaßnahme kommen bereits angesprochene VPNs zwischen Ladestation/Internet-Modem und Internet-Provider/CPMS in Frage – mit allen Nachteilen wie Kosten, Komplexität, Rechenaufwand, usw.
i) **(-) Fehlender direkter Zugriff durch Kund_innen und Missbrauch von Steuersignalen:** die Notwendigkeit sofortiger Abschaltung im Notfall (bei Überlast) wird durch Mobilfunk und die entsprechenden Verzögerungen nicht gewährleistet. Als „Not-Aus“ sollten daher andere, redundante Lösungen überlegt werden. Eine Option wäre z.B. die Verwendung

von Steuersignalen ähnlich dem „Nachtstrom“ in Stromnetzen. Diese Steuersignale sind jedoch zur Zeit nicht gesichert und können daher theoretisch von Angreifern missbraucht werden.

Die Nachteile der verbleibenden Anwendungsfälle AF0, AF2 Variante a OHNE VLAN-Trennung der Ladestation, sowie AF2 Variante b und AF3 wiegen deren Vorteile nach Einschätzung der Studienautor_innen nicht auf.

3. **AF0 bietet keine Möglichkeit der Steuerung für den CPO. Aufgrund der verpflichtenden, bidirektionalen, digitalen Schnittstelle** werden regulatorische Auflagen für den Anschluss der Ladestation jedoch in Kürze eine Vernetzung neuer Ladestationen vorschreiben als eine Voraussetzung für externe Steuerung (gemäß Kapitel 5.9.2 von [37]).
4. **AF2 Variante a (ohne VLAN-Trennung) sowie AF2 Variante b** (Details zu beiden AF in Kapitel 5.4.3**) gefährden die Sicherheit von Ladestationen und Privatsphäre von Kund_innen.** Möglicherweise kompromittierte Geräte im LAN der Kund_innen können die Ladestation angreifen und/oder mögliche Angriffsmöglichkeiten prüfen. In Variante a kann eine host-basierte Firewall auf der Ladestation gegen lokale Angriffe schützen, da lokale Geräte nicht auf die Ladestation zugreifen müssen. Bei Variante b müssen lokale Geräte zugreifen können, d.h. diese Einschränkung fällt. CPOs können in beiden Varianten die Ladestation als Jump Host verwenden um die Privatsphäre von Kund_innen zu gefährden, das LAN auszukundschaften, Geräte zu entdecken, Profile zu erstellen, usw.
5. **AF3** (Details in Kapitel 5.4.4) **gefährdet die Sicherheit von Ladestationen und Privatsphäre von Kund_innen und erhöht die Angriffsfläche.** Wesentlicher Vorteil von AF3 ist die Redundanz: der CPO kann sowohl über Mobilfunk als auch über das Kund_innen-LAN auf die Ladestation zugreifen. Allerdings bedingt dieser Vorteil eine signifikante Gefährdung der Privatsphäre von Kund_innen durch den CPO: die Ladestation hängt im LAN der Kund_innen – der CPO kann unbemerkt und nicht von Kund_innen kontrollierbar über Mobilfunk auf die Ladestation zugreifen und über deren LAN-Schnittstelle der Ladestation das Kund_innen-LAN auskundschaften. Weiters ist die Ladestation aus dem LAN (von kompromittierten Geräten im Kund_innen-LAN) angreifbar und der CPO bzw. das CPMS hat wegen der variablen IP-Adresse der Kund_innen-Internetanbindung ebenfalls eine erhöhte Angriffsfläche. Details betreffend die erhöhte Angriffsfläche entsprechen der Beschreibung unter Punkt 2.h der empfohlenen Variante a von AF2 mit VLAN-Trennung, „Herausforderungen beim Schutz des CPO/CPMS“.

6.3 Schlussfolgerung

Die Verwendung von OCPP für die Steuerung von Ladestationen von Kund_innen durch CPOs ist grundsätzlich möglich. Folgende Empfehlungen sollen die Sicherheit sicherstellen – detaillierte Beschreibungen der entsprechenden Gefährdungen finden sich in Kapitel 5.4.

6.3.1 Notwendige Annahme: „Missing Trust“

Grundlage der Architektur aus CPO-Sicht muss die Annahme sein, dass jede bei Kund_innen installierte Ladestation potentiell kompromittiert sein kann, wie auch jede andere Komponente (wie z.B. Router oder PC) im Kund_innen-LAN. Physischer Zugriff auf eine Komponente ist im sicherheitstechnischen Kontext gleichzusetzen mit der Möglichkeit der Kompromittierung. Die Infrastruktur des CPO bzw. das CPMS muss entsprechend geplant und durch Monitoring begleitet werden. Ziel ist, dass eine kompromittierte Ladestation weder andere Kund_innen noch die Sicherheit der Infrastruktur des CPO gefährden kann.

6.3.2 Ende-zu-Ende TLS-Verschlüsselung

Wie bei jedem Dienst über das öffentliche Internet öffnet so eine Ladstationssteuerung Angriffsflächen, die je nach Anwendungsfall unterschiedlich ausfallen. Zwingend notwendig sind geeignete Architekturen und Sicherheitsmaßnahmen, beginnend mit einer Ende-zu-Ende Absicherung der Kommunikation durch geeignete TLS-Versionen (1.2., 1.3) mit geeigneten Ciphers (die ECDSA-Varianten gemäß der OCPP-Standards werden empfohlen, EdDSA ist eine zur Zeit vielversprechende Entwicklung) und einer geeigneten Infrastruktur für Minimierung der Angriffsflächen. Diese Vorgaben entsprechen den OCPP Security Profiles 3 bzw. notfalls 2. Die Verwendung oder Unterstützung der von OCPP 1.6 für Rückwärtskompatibilität vorgesehenen TLS-Versionen 1.0 und 1.1 ist aus den in Kapitel 5.4.1.2 genannten Gründen ausnahmslos zu streichen und keinesfalls zulässig.

6.3.3 Bewertung Anwendungsfälle

Die beste Sicherheit mit den kleinsten Angriffsflächen für Ladestation und CPO, sowie die geringste Gefährdung der Privatsphäre von Kund_innen bietet nach Einschätzung der Studienautor_innen der Anwendungsfall AF1, Anbindung der Ladestation über Mobilfunk mit privaten APNs, festen IP-Adressen, Intra-APN-Sicherheitsmaßnahmen und OCPP Security Profile 3. Vertretbar ist – vorbehaltlich der technischen Realisierbarkeit im Einzelfall – mit etwas höherer Angriffsfläche, vor allem für den CPO, auch Anwendungsfall AF2 Variante a mit VLAN-basierter Trennung der Ladestation. Sowohl bei AF2 Variante a ohne VLAN-basierte Trennung der Ladestation, als auch bei AF2 Variante b und AF3 besitzt der CPO die technische Voraussetzung um die Privatsphäre von Kund_innen (absichtlich oder unabsichtlich) zu gefährden. Desgleichen vergrößern diese drei letztgenannten Anwendungsfälle die Angriffsflächen und reduzieren die Abwehrmöglichkeiten deutlich, sowohl für Ladestation als auch für CPO. Letztere Aussage gilt auch für die Verwendung von OCPP Security Profile 2 mit den genannten Zusatzbedingungen (Angreifer ohne Möglichkeit, den eindeutigen Ladestations-Schlüssel herauszufinden) statt dem empfohlenen OCPP Security Profile 3.

6.3.4 Herausforderung: Inbetriebnahme

Als wesentliche Herausforderung und gleichzeitig höchstes Gefährdungspotential durch Angriffe sieht diese Studie eine erstmalige, sichere Inbetriebnahme der Ladestation, evtl. mit ZeroConf (Plug&Play) Anforderungen. Die Zertifikats-Infrastruktur für den Aufbau einer sicheren TLS-Verbindung hängt von einer ausreichend genauen Uhrzeit ab. Technisch gesehen sollte eine batteriegestützte Uhr in der Ladestation auch bei mehrjähriger Lagerung problemlos die notwendige Genauigkeit erreichen können. Allerdings müssen die Zertifikate hinreichend lange gültig sein. Die Erstellung und Prüfung eines entsprechenden Sicherheitskonzepts mit Schwerpunkt Uhrzeit und Zertifikate für die erstmalige Installation bzw. Inbetriebnahme von Ladestationen wird dringend empfohlen. Sobald die Ladestation einmal eine gültige und überprüfte TLS-Verbindung zum CPMS aufgebaut hat, bietet OCPP die notwendigen Mechanismen um sichere Updates von Zertifikaten, Firmware-Images usw. durchzuführen.

6.3.5 Mögliche Reaktionszeiten auf Steuerbefehle

Die Reaktionszeit einer Ladestation auf einen Steuerungsbefehl (SetChargingProfile) des CPMS für Anwendungsfall AF1 (Mobilfunk-Anbindung) hängt von mehreren Parametern ab. Den größten Anteil daran hat – abhängig von der verwendeten Technologie – die Laufzeit der Steuerungsnachrichten über das Kommunikationsnetz sowie die (nicht quantifizierbare, da für jedes Modell unterschiedliche) Bearbeitungszeit der Ladestation. Die Messergebnisse in realen Setups für M2M SIM-Karten mit privatem APN in Kapitel 4.3 und 4.4 zeigen, dass bei der Verwendung von Mobilfunk u.a. die Funktechnologie, die Länge der Pausen zwischen zwei aufeinanderfolgenden Übertragungen, sowie die Größe von Steuerungsnachrichten deren Laufzeit signifikant beeinflussen. Die Messungen setzen eine bereits aufgebaute, vorhandene TLS-Verbindung und die Verwendung von OCPP-J mit

JSON/WebSocket Kommunikation voraus, bei 30 Sekunden Pause nach vorhergehenden Übertragungen. Für diese Konfiguration kann als Größenordnung für die Übertragungszeit einer 1500 Byte großen Steuerungsnachricht vom CPMS an eine Ladestation (d.h. Einweg-Verzögerung) von folgenden Werten als untere Schranke ausgegangen werden: ca. 580 ms Laufzeit für 4G Netze, 1700ms (3G) bzw. 1500ms (2G).

Die Antwort bzw. Rückmeldung der Ladestation (Round-Trip Delay, d.h. Laufzeit von Steuerbefehl plus Rückmeldung) erhält das CPMS frühestens (da zuzüglich der nicht berücksichtigten Bearbeitungszeit der Ladestation) ca. 0,6 Sekunden für 4G Netze, 1,8 Sekunden (3G) bzw. 3 Sekunden (2G) nach Absenden seines Steuerungsbefehls.

Die hohe Verzögerung für den Steuerbefehl erklärt sich in der Optimierung der Netze – nach kurzer Inaktivität (ein paar Sekunden reichen) werden Ressourcen freigegeben. Das Mobilfunknetz muss beim einlangenden Paket des Steuerbefehls die Ressourcen wieder zuweisen – was bei 3G offensichtlich langwieriger ist als bei 2G. Die Laufzeit der Rückantwort ist nach der bereits erfolgten Zuweisung der Ressourcen um Größenordnungen kürzer (35ms für 4G, 100ms für 3G, 1500ms für 2G) - mit Ausnahme von 2G, begründet durch geringe Kapazitäten im Uplink.

Bei anderen Technologien der Kommunikationsnetze (Kabel oder VDSL) ist von deutlich geringeren Antwortzeiten auszugehen, von 15-100ms. Aufgrund der vielen unterschiedlichen Technologien und vor allem Parametrierungen (Übertragungskapazitäten abhängig vom jeweiligen Angebot des Internet-Providers) sowie der Präferenz für Anwendungsfall AF1 wurde von konkreten Messungen AF2 abgesehen.

Die Schlussfolgerung bezüglich Reaktionszeit bei Steueranforderung des CPMS ist, dass diese Zeit, unabhängig von der verwendeten Technologie, in der Größenordnung von etwa 3 Sekunden liegen sollte – mit deutlich niedrigeren Werten bei 3G, 4G und kabelgebundenen Technologien. Für den typischen Anwendungsfall der Stabilisierung von Netzen sind die 3 Sekunden in vielen Fällen anwendbar – falls bessere Reaktionszeiten notwendig sind, müssen andere Technologien als 2G zum Einsatz kommen.

7 Bibliografie

[1] „E-Autos in Österreich - Neuzulassungen“. https://oesterreichsenergie.at/downloads/grafiken/detailseite/e-autos-in-oesterreich-neuzulassungen (zugegriffen 17. Februar 2023).

[2] „Anzahl an E-Autos in Österreich“. https://oesterreichsenergie.at/downloads/grafiken/detailseite/anzahl-an-e-autos-in-oesterreich (zugegriffen 17. Februar 2023).

[3] „CCC | Chaos Computer Club hackt Ladesäulen“. https://www.ccc.de/de/updates/2017/e-motor (zugegriffen 17. Februar 2023).

[4] „Downloads - Open Charge Alliance“. https://www.openchargealliance.org/downloads/ (zugegriffen 27. Jänner 2023).

[5] „RIS - Festlegung einheitlicher Standards beim Infrastrukturaufbau für alternative Kraftstoffe - Bundesrecht konsolidiert, Fassung vom 17.02.2023“. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010261 (zugegriffen 17. Februar 2023).

[6] „OSI-Modell“, *Wikipedia*. 8. Februar 2023. Zugegriffen: 17. Februar 2023. [Online]. Verfügbar unter: https://de.wikipedia.org/w/index.php?title=OSI-Modell&oldid=230670038

[7] „IEEE Standards Association“, *IEEE Standards Association*. https://standards.ieee.org (zugegriffen 22. Februar 2023).
[8] R. W. Shirey, „Internet Security Glossary, Version 2“, Internet Engineering Task Force, Request for Comments RFC 4949, Aug. 2007. doi: 10.17487/RFC4949.
[9] M. Neaimeh und P. B. Andersen, „Mind the gap- open communication protocols for vehicle grid integration“, *Energy Inform.*, Bd. 3, Nr. 1, S. 1, Feb. 2020, doi: 10.1186/s42162-020-0103-1.
[10] „Normenlandschaft für die Elektromobilität“, *FfE*. https://www.ffe.de/veroeffentlichungen/normenlandschaft_fuer_die_elektromobilitaet/ (zugegriffen 20. Februar 2023).
[11] „IEC TC 69 Dashboard > Projects: Work programme, Publications, Maintenance cycle, Project files, TC/SC in figures“. https://www.iec.ch/ords/f?p=103:38:615145347520773::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1255,20,100392 (zugegriffen 20. Februar 2023).
[12] „IEC TC 69 Dashboard > Projects: Work programme, Publications, Maintenance cycle, Project files, TC/SC in figures“. https://www.iec.ch/ords/f?p=103:38:615145347520773::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1255,20,100391 (zugegriffen 20. Februar 2023).
[13] „IEC TC 69 Dashboard > Projects: Work programme, Publications, Maintenance cycle, Project files, TC/SC in figures“. https://www.iec.ch/ords/f?p=103:38:615145347520773::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1255,20,100390 (zugegriffen 20. Februar 2023).
[14] Directorate-General for Mobility and Transport (European Commission), *Mapping of the discussion concerning standards and protocols for communication exchange in the electromobility ecosystem*. LU: Publications Office of the European Union, 2022. Zugegriffen: 20. Februar 2023. [Online]. Verfügbar unter: https://data.europa.eu/doi/10.2832/6763
[15] R. Metere, Z. Pourmirza, S. Walker, und M. Neaimeh, „An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure“. arXiv, 16. September 2022. doi: 10.48550/arXiv.2209.07842.
[16] R. Metere, M. Neaimeh, C. Morisset, C. Maple, X. Bellekens, und R. M. Czekster, „Securing the Electric Vehicle Charging Infrastructure“. arXiv, 6. Juli 2022. doi: 10.48550/arXiv.2105.02905.
[17] B. R. Anderson und J. T. Johnson, „Securing Vehicle Charging Infrastructure Against Cybersecurity Threats.“, Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), SAND2020-0818C, Jän. 2020. Zugegriffen: 15. Jänner 2023. [Online]. Verfügbar unter: https://www.osti.gov/biblio/1763166
[18] N. Bhusal, M. Gautam, und M. Benidris, „Cybersecurity of Electric Vehicle Smart Charging Management Systems“. arXiv, 17. August 2020. doi: 10.48550/arXiv.2008.07511.
[19] F. Steffen und F. Rainer, „Electric Vehicle Charging Infrastructure – Security Considerations and Approaches“, *Fourth Int. Conf. Evol. Internet*, S. 58--64, 2012.
[20] Z. Pourmirza und S. Walker, „Electric Vehicle Charging Station: Cyber Security Challenges and Perspective“, in *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*, Aug. 2021, S. 111–116. doi: 10.1109/SEGE52446.2021.9535052.
[21] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, und C. Douligeris, „Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)“, *IEEE Commun. Surv. Tutor.*, Bd. 24, Nr. 3, S. 1504–1533, 2022, doi: 10.1109/COMST.2022.3184448.
[22] C. Alcaraz, J. Lopez, und S. Wolthusen, „OCPP Protocol: Security Threats and Challenges“, *IEEE Trans. Smart Grid*, Bd. 8, Nr. 5, S. 2452–2459, Sep. 2017, doi: 10.1109/TSG.2017.2669647.
[23] D. Sklyar, „ChargePoint Home security research“, Kaspersky Lab Security Services, 2018. [Online]. Verfügbar unter: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/12/13084354/ChargePoint-Home-security-research_final.pdf
[24] M. Witt, *Zero Trust Charge Points Kommunikation / vorgelegt von: Markus Witt*. 2021. Zugegriffen: 31. Jänner 2023. [Online]. Verfügbar unter: http://pub.fh-campuswien.ac.at/obvfcwhsacc/6260844

[25] T. Alladi, V. Chamola, B. Sikdar, und K.-K. R. Choo, „Consumer IoT: Security Vulnerability Case Studies and Solutions“, *IEEE Consum. Electron. Mag.*, Bd. 9, Nr. 2, S. 17–25, März 2020, doi: 10.1109/MCE.2019.2953740.
[26] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, und N. Ghani, „Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations“, *IEEE Commun. Surv. Tutor.*, Bd. 21, Nr. 3, S. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.
[27] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, und P. Faruki, „Network Intrusion Detection for IoT Security Based on Learning Techniques“, *IEEE Commun. Surv. Tutor.*, Bd. 21, Nr. 3, S. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.
[28] L. Xiao, X. Wan, X. Lu, Y. Zhang, und D. Wu, „IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?“, *IEEE Signal Process. Mag.*, Bd. 35, Nr. 5, S. 41–49, Sep. 2018, doi: 10.1109/MSP.2018.2825478.
[29] M. binti Mohamad Noor und W. H. Hassan, „Current research on Internet of Things (IoT) security: A survey“, *Comput. Netw.*, Bd. 148, S. 283–294, Jän. 2019, doi: 10.1016/j.comnet.2018.11.025.
[30] A. Jacobsson, M. Boldt, und B. Carlsson, „A risk analysis of a smart home automation system“, *Future Gener. Comput. Syst.*, Bd. 56, S. 719–733, März 2016, doi: 10.1016/j.future.2015.09.003.
[31] G. Dorai, E. A. Williams, H. Chi, und R. A. Alo, „‚Is your Smart Home a Secure Home?‘ - Analysis of Smart Home Breaches and an Approach for Vulnerability Analysis and Device Isolation“, in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, Juni 2020, S. 1–6. doi: 10.1109/WF-IoT48130.2020.9221420.
[32] B. Ali und A. I. Awad, „Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes“, *Sensors*, Bd. 18, Nr. 3, S. 817, März 2018, doi: 10.3390/s18030817.
[33] E. Fernandes, J. Jung, und A. Prakash, „Security Analysis of Emerging Smart Home Applications“, in *2016 IEEE Symposium on Security and Privacy (SP)*, Mai 2016, S. 636–654. doi: 10.1109/SP.2016.44.
[34] E. Zeng, S. Mare, und F. Roesner, „End user security & privacy concerns with smart homes“, in *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, in SOUPS ’17. USA: USENIX Association, Juli 2017, S. 65–80.
[35] N. Komninos, E. Philippou, und A. Pitsillides, „Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures“, *IEEE Commun. Surv. Tutor.*, Bd. 16, Nr. 4, S. 1933–1954, 2014, doi: 10.1109/COMST.2014.2320093.
[36] „EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex“. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504 (zugegriffen 13. April 2023).
[37] T. Verteilernetzanschluss, „Technische und organisatorische Regeln für Betreiber und Benutzer von Netzen“.
[38] A. Gordon, „Russian Electric Vehicle Chargers Hacked, Tell Users ‘PUTIN IS A DICKHEAD’“, *Vice*, 28. Februar 2022. https://www.vice.com/en/article/akvya5/russian-electric-vehicle-chargers-hacked-tell-users-putin-is-a-dickhead (zugegriffen 22. Februar 2023).
[39] „RIS - Elektrizitätswirtschafts- und -organisationsgesetz 2010 - Bundesrecht konsolidiert, Fassung vom 22.02.2023“. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007045 (zugegriffen 22. Februar 2023).
[40] „E-Control - SmartMeter Fragen und Antworten“. Zugegriffen: 22. Februar 2023. [Online]. Verfügbar unter: https://www.e-control.at/documents/1785851/1811582/Fragen-Antworten_Smart-Meter_Januar_2019.pdf/ec97d936-3a50-8e29-8ea0-569abaac9065?t=1548350828909
[41] „OCPP 1.6, Protocols, Home - Open Charge Alliance“. https://www.openchargealliance.org/protocols/ocpp-16/ (zugegriffen 23. Februar 2023).
[42] „OCPP enables electric vehicle grid integration | Ampcontrol“. https://www.ampcontrol.io/post/what-are-ocpp-iec-63110-iso-15118-and-how-do-they-relate-to-v2g (zugegriffen 20. Februar 2023).

[43] E. Rescorla und T. Dierks, „The Transport Layer Security (TLS) Protocol Version 1.2“, Internet Engineering Task Force, Request for Comments RFC 5246, Aug. 2008. doi: 10.17487/RFC5246.
[44] E. Rescorla, „The Transport Layer Security (TLS) Protocol Version 1.3“, Internet Engineering Task Force, Request for Comments RFC 8446, Aug. 2018. doi: 10.17487/RFC8446.
[45] K. Moriarty und S. Farrell, „Deprecating TLS 1.0 and TLS 1.1“, Internet Engineering Task Force, Request for Comments RFC 8996, März 2021. doi: 10.17487/RFC8996.
[46] „Enhanced security for OCPP 1.6 - Open Charge Alliance“. https://www.openchargealliance.org/news/enhanced-security-for-ocpp-16/ (zugegriffen 27. Oktober 2020).
[47] „Sicherheitslücken bei BMW Connected Drive | ADAC“. https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/sicherheitsluecken-bmw-connected-drive/ (zugegriffen 27. Jänner 2023).
[48] „OCPP 2.0.1, Protocols, Home - Open Charge Alliance“. https://www.openchargealliance.org/protocols/ocpp-201/ (zugegriffen 27. Jänner 2023).
[49] „SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)“. https://www.w3.org/TR/soap12/ (zugegriffen 23. Februar 2023).
[50] A. Melnikov und I. Fette, „The WebSocket Protocol“, Internet Engineering Task Force, Request for Comments RFC 6455, Dez. 2011. doi: 10.17487/RFC6455.
[51] J. Fabini, T. Zseby, und M. Hirschbichler, „Representative delay measurements (RDM): facing the challenge of modern networks“, in *Proceedings of the 8th International Conference on Performance Evaluation Methodologies and Tools*, in VALUETOOLS ’14. Brussels, BEL: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Dezember 2014, S. 17–24. doi: 10.4108/icst.Valuetools.2014.258181.
[52] E. Barker und A. Roginsky, „Transitioning the Use of Cryptographic Algorithms and Key Lengths“, National Institute of Standards and Technology, NIST Special Publication (SP) 800-131A Rev. 2, März 2019. doi: 10.6028/NIST.SP.800-131Ar2.
[53] „Algorithms, key size and parameters report 2014“, *ENISA*. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 (zugegriffen 29. März 2023).
[54] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, und P. E. Hoffman, „Specification for DNS over Transport Layer Security (TLS)“, Internet Engineering Task Force, Request for Comments RFC 7858, Mai 2016. doi: 10.17487/RFC7858.
[55] P. E. Hoffman und P. McManus, „DNS Queries over HTTPS (DoH)“, Internet Engineering Task Force, Request for Comments RFC 8484, Okt. 2018. doi: 10.17487/RFC8484.
[56] P. E. Hoffman, „DNS Security Extensions (DNSSEC)“, Internet Engineering Task Force, Request for Comments RFC 9364, Feb. 2023. doi: 10.17487/RFC9364.
[57] R. T. Fielding, Y. Lafon, und J. Reschke, „Hypertext Transfer Protocol (HTTP/1.1): Range Requests“, Internet Engineering Task Force, Request for Comments RFC 7233, Juni 2014. doi: 10.17487/RFC7233.
[58] R. T. Fielding, M. Nottingham, und J. Reschke, „HTTP Semantics“, Internet Engineering Task Force, Request for Comments RFC 9110, Juni 2022. doi: 10.17487/RFC9110.