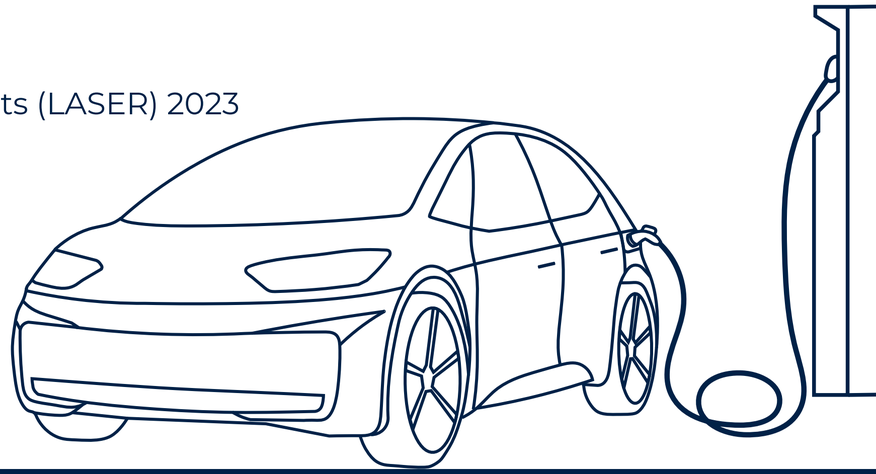
Evaluating Wireless Attacks Against CCS Electric Vehicle Charging

Sebastian Köhler[‡†], Richard Baker[‡†], Martin Strohmeier[*], Ivan Martinovic[‡]

[‡]University of Oxford, [*]armasuisse Science + Technology

Workshop on Learning from Authoritative Security Experiment Results (LASER) 2023

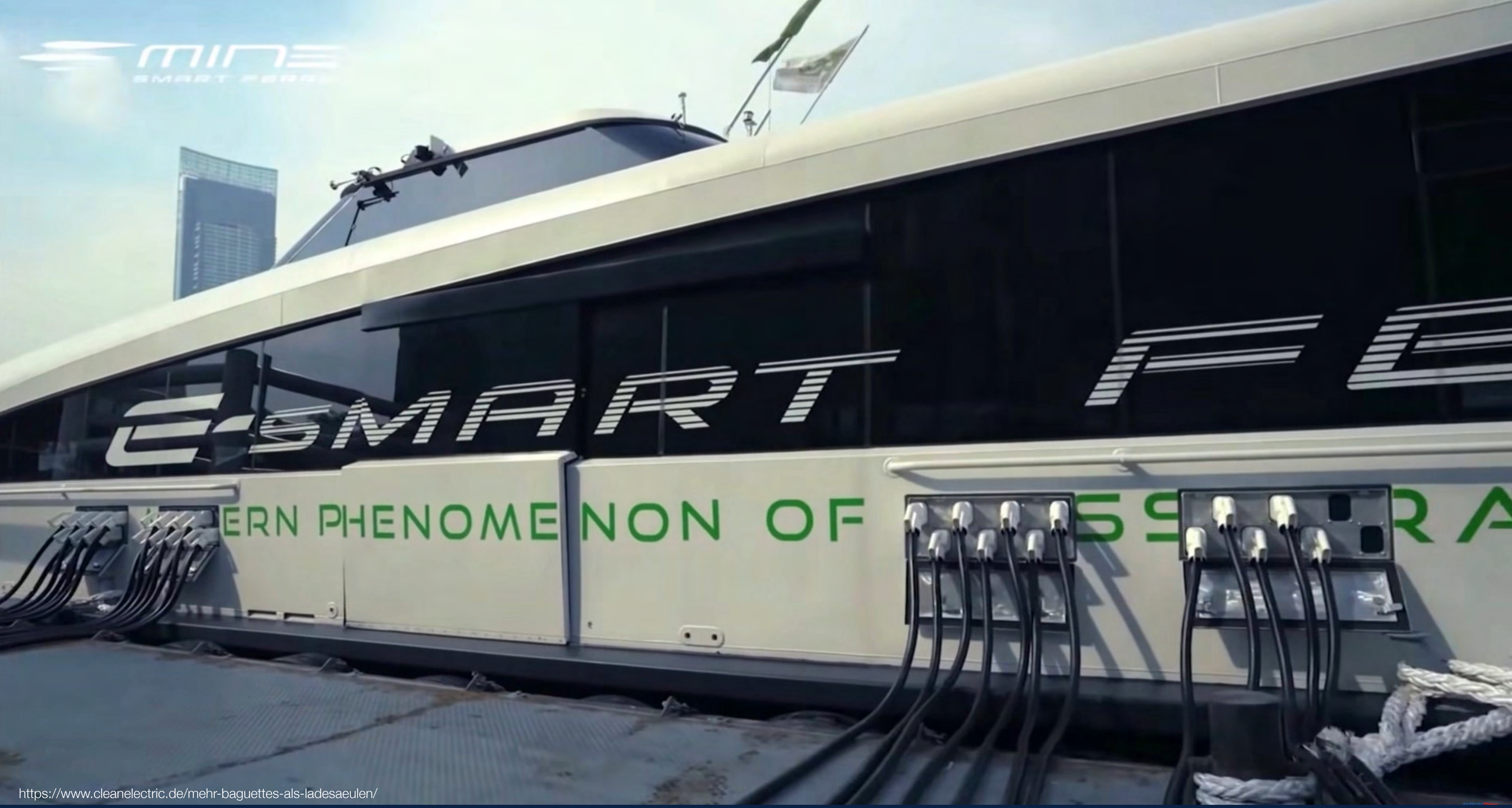


† Both authors contributed equally to this paper.

https://www.enbw.com/unternehmen/presse/groesster-enbw-schnellladepark-eroeffnet.html

https://www.ingenieur.de/technik/fachbereiche/e-mobilitaet/neue-initiative-fuer-den-aufbau-einer-ladeinfrastruktur-fuer-e-lkw/


10
11
12
13
14
15
16
17
Credit: Hamburger Hochbahn AG

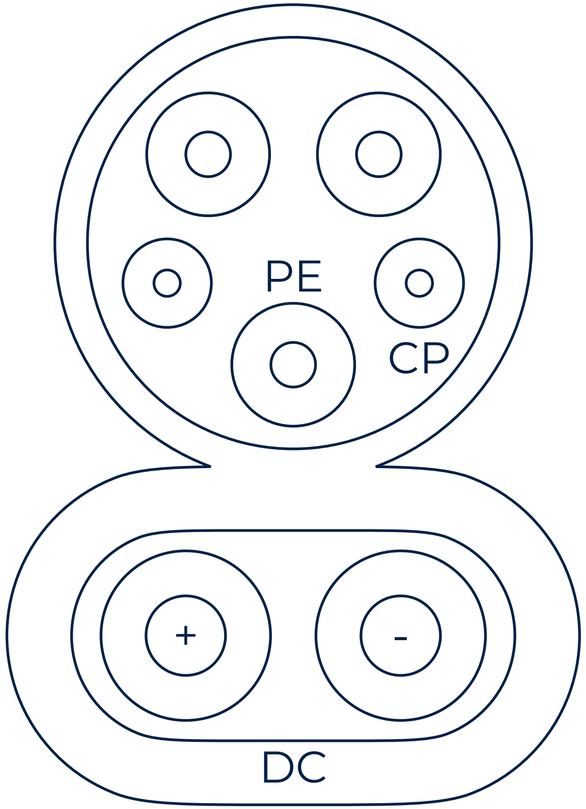


https://www.cleanelectric.de/mehr-baguettes-als-ladesaeulen/

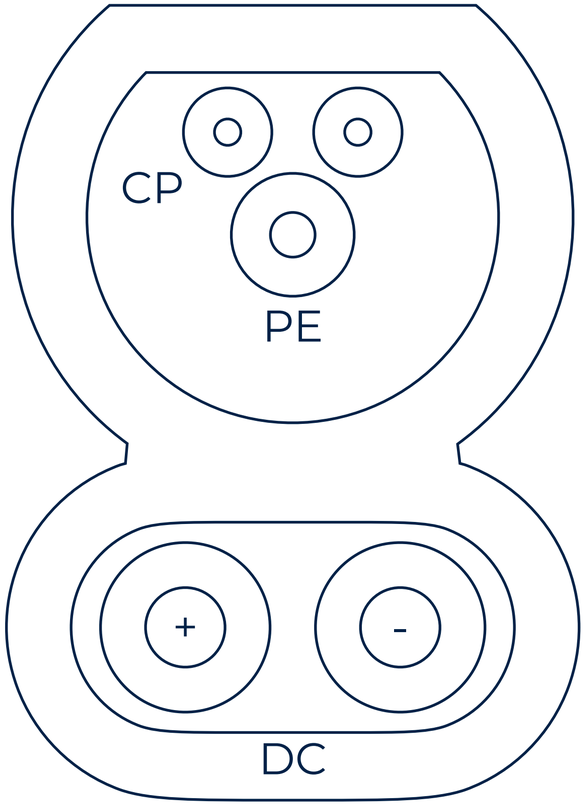
https://wall.alphacoders.com/big.php?i=933709

https://cdn.motor1.com/images/mgl/g3WJm/s2/efacec-s-first-350-kw-ccs-combo-dc-fast-chargers-already-up-amp-running.jpg

Combined Charging System (CCS)

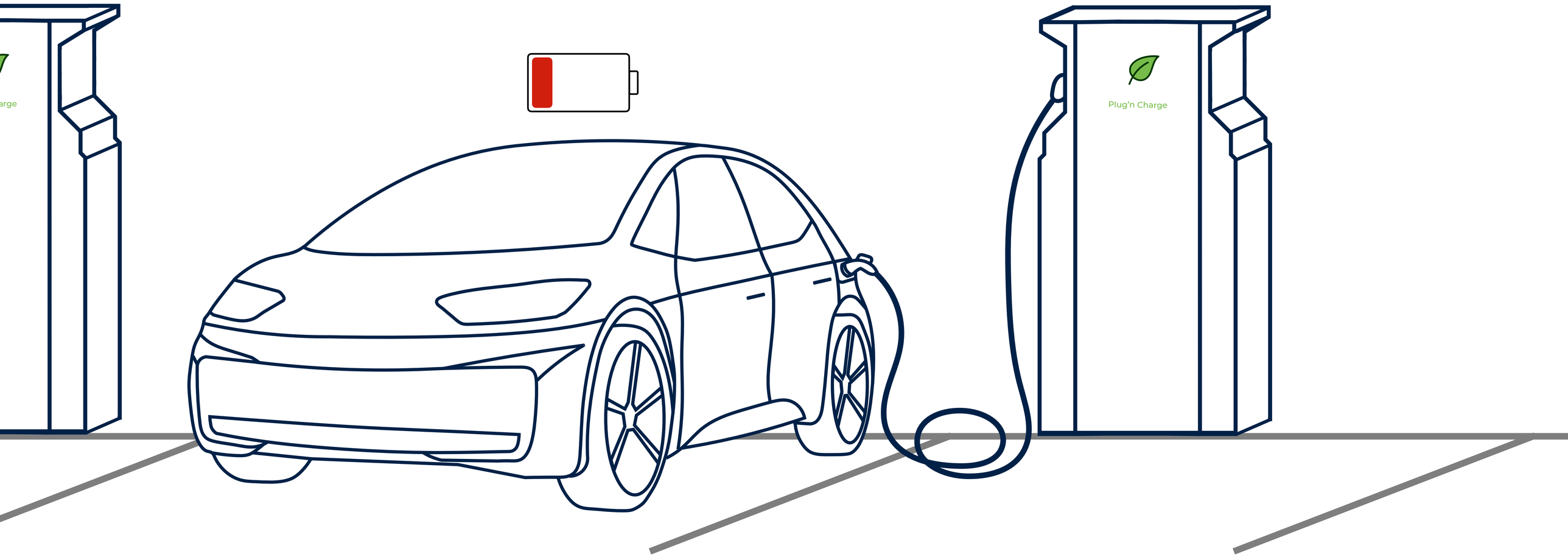


CCS Combo 1 (US)



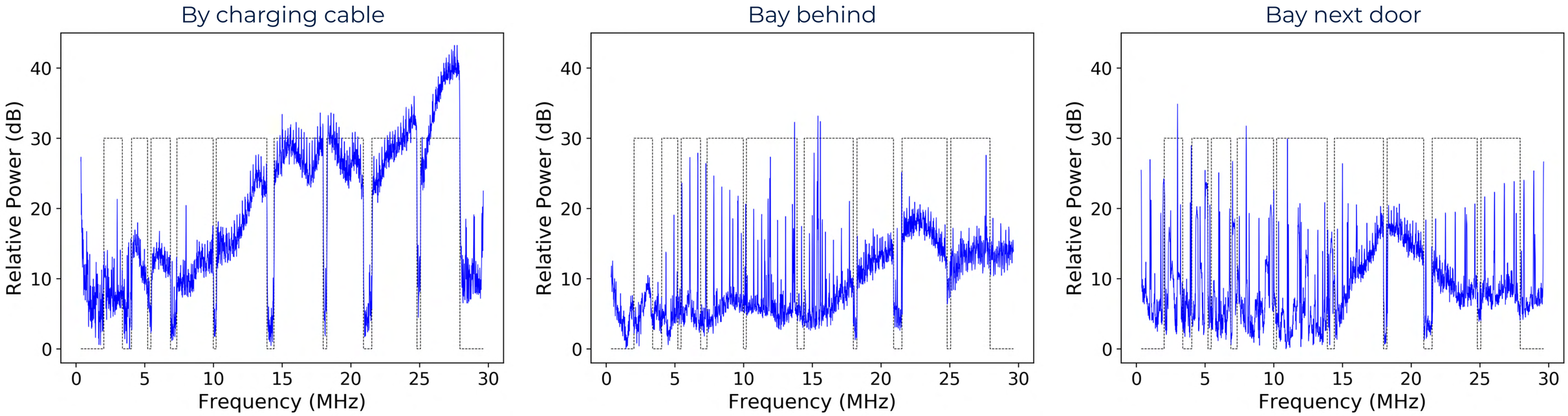
CCS Combo 2 (EU)

CCS Power-Line Communication



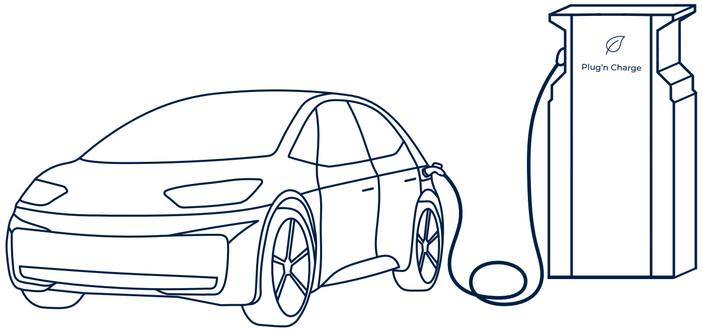
Previous Work on EV Security

"[The] use of PLC in EV charging and the design of the CCS standard lead to a uniquely high-quality, ***unintentional wireless channel****." [1]*

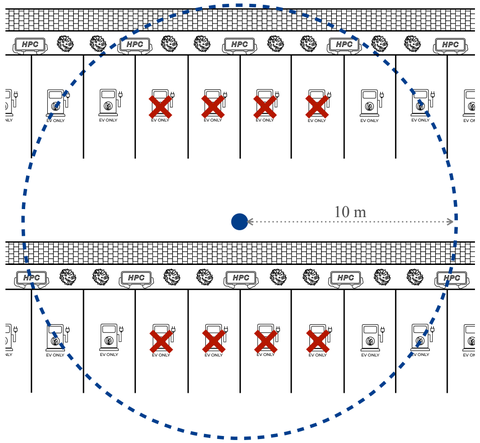


[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

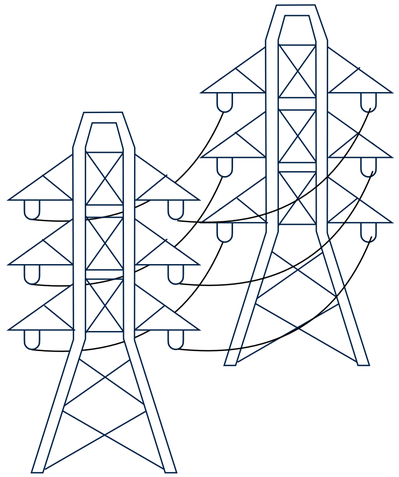
Threat Model: Goals



Individual Vehicle

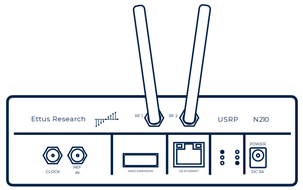


Fleet Denial

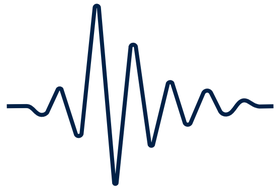


Unspecific Disruption

Threat Model: Capabilities

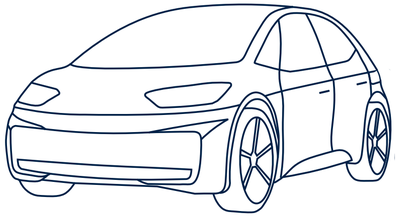


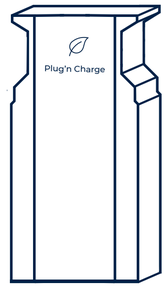
Access to off-the-shelf equipment



Little to no DSP knowledge

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)





Without CSMA/CA

With CSMA/CA

Clear to send?

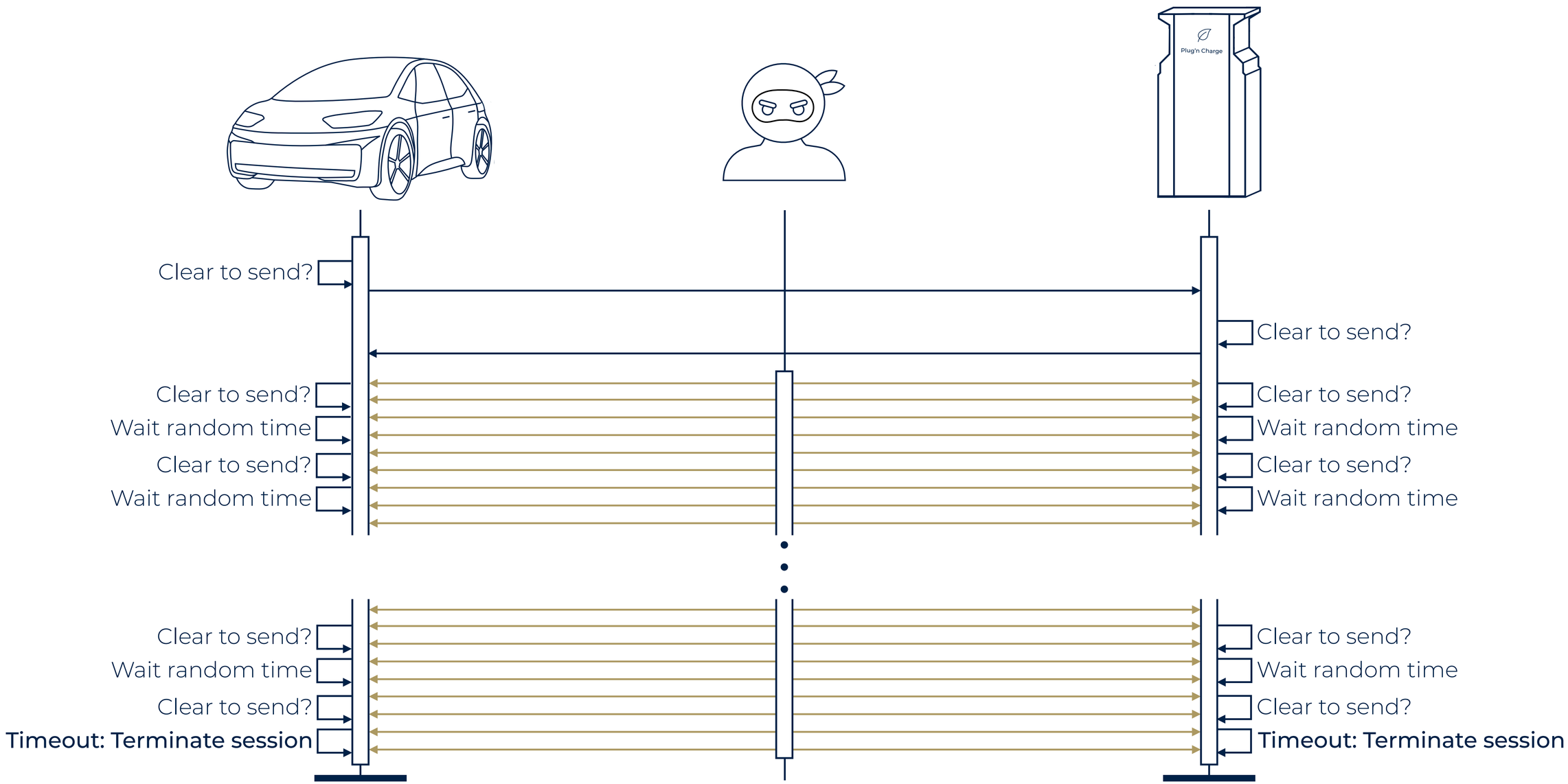
Clear to send?

Clear to send?

Wait random time

Clear to send?

Exploiting CSMA/CA



Brokenwire Attack: Wireless Exploitation of CSMA/CA

*“The receiver shall be able to **detect the presence** of Preamble Symbols […]: When the desired Preamble Symbol waveform present at the receiver has a signal power of -35 dBm and is corrupted by Gaussian noise producing a **total SNR of 2 dB** at the receiver terminal.“ [2]*

+

*“[The] use of PLC in EV charging and the design of the CCS standard lead to a uniquely high- quality, **unintentional wireless channel**.“ [1]*

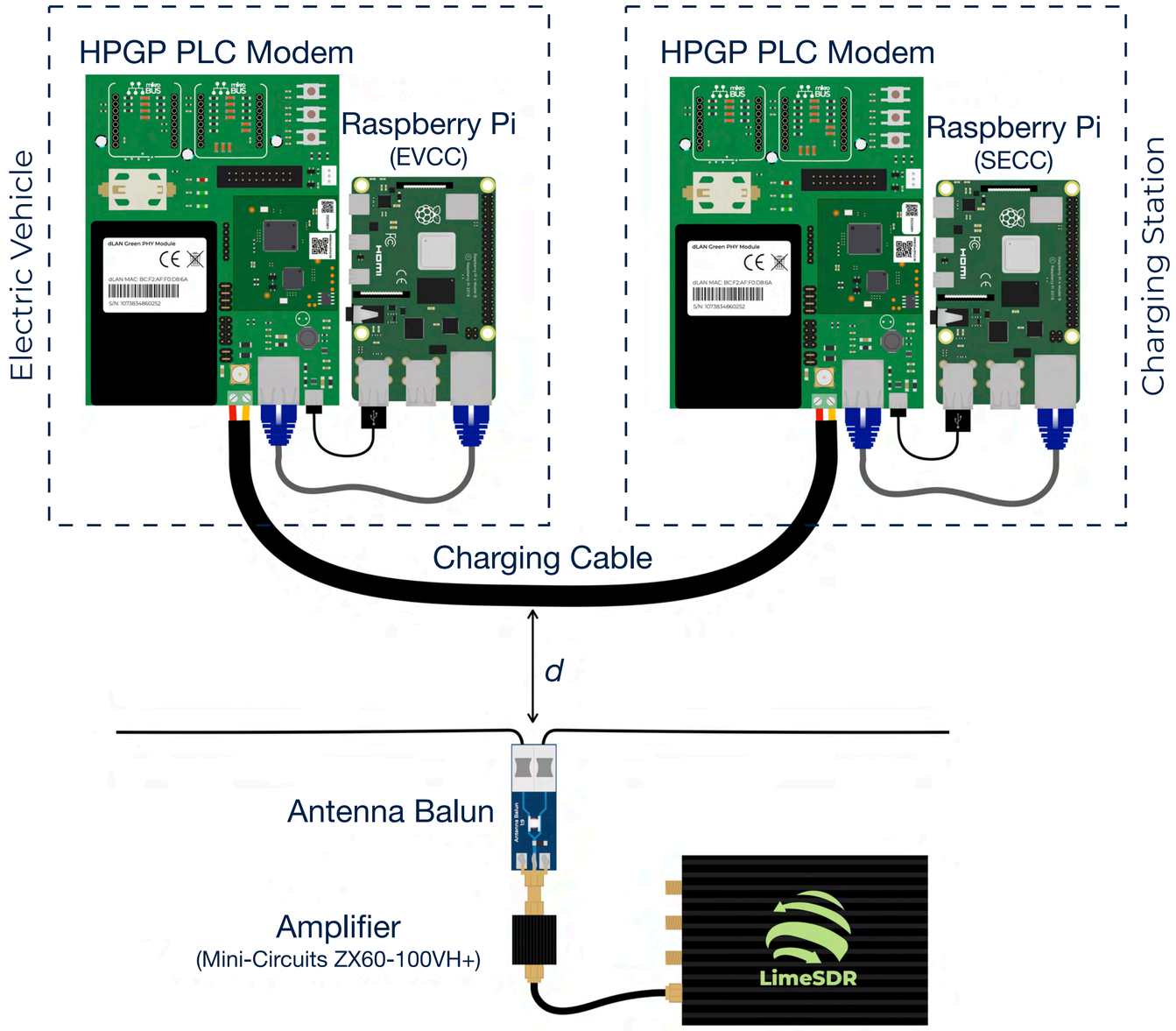
=

Can we use electromagnetic waves to wirelessly disrupt CCS electric vehicle charging from a distance?

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.

[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.

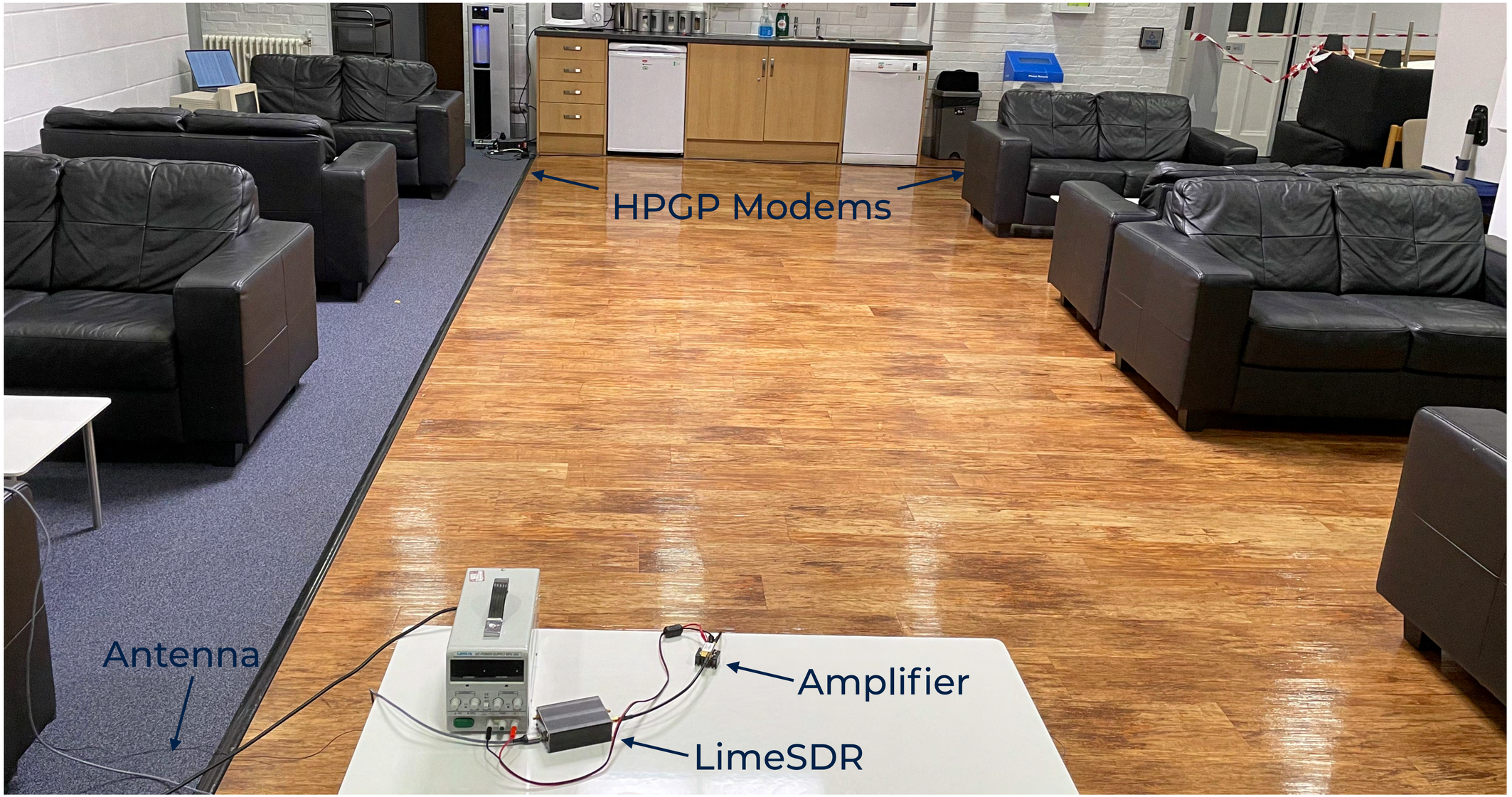
Lab Testing: Experimental Setup



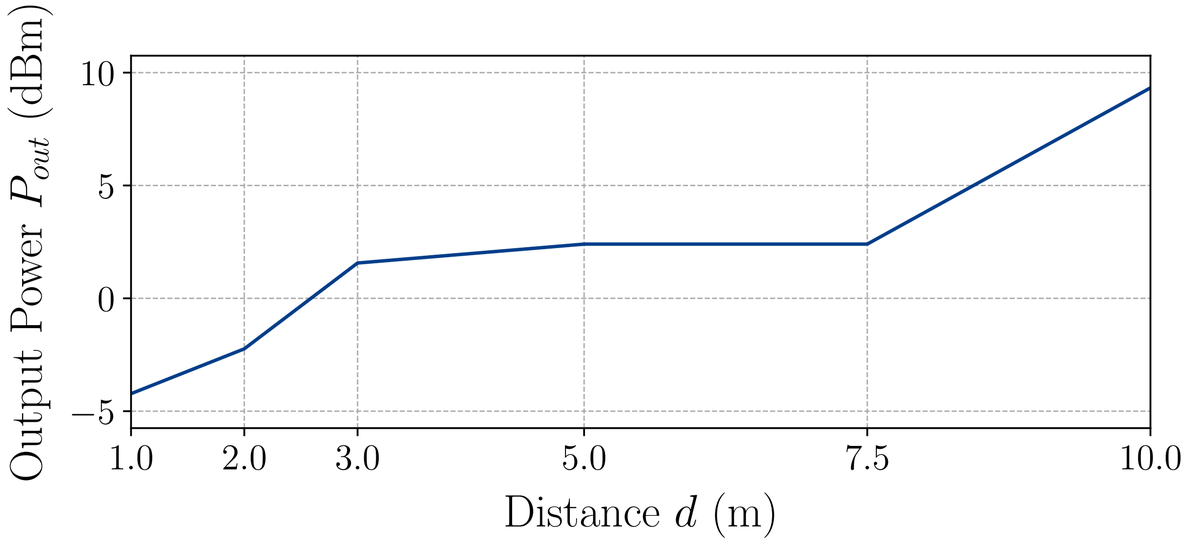
Lab Testing: Method

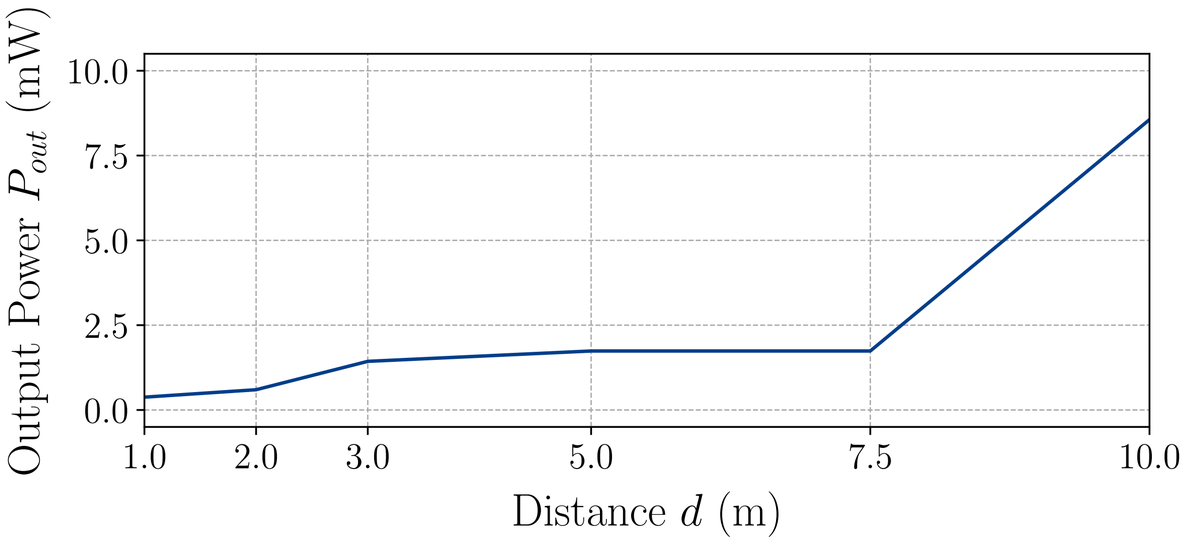
- We set up a UDP transmission between two RaspberryPis connected via the PLC modems.
- Without an attacker, packet loss was 0%.
- We expected that injecting preambles into the communication tricks the nodes into thinking the medium is busy, resulting in a reduced throughput.
- By slowly increasing the transmission power, the number of successfully injected preambles increased.
- Eventually, the nodes stopped communicating and the packet loss reached 100%.
- We conducted the experiment for different distances to measure the required transmission power for a given distance.
- We repeated the experiments multiple times to ensure that uncontrollable environmental factors are taken into account.

Lab Testing: Power vs. Distance



Lab Testing: Power vs. Distance

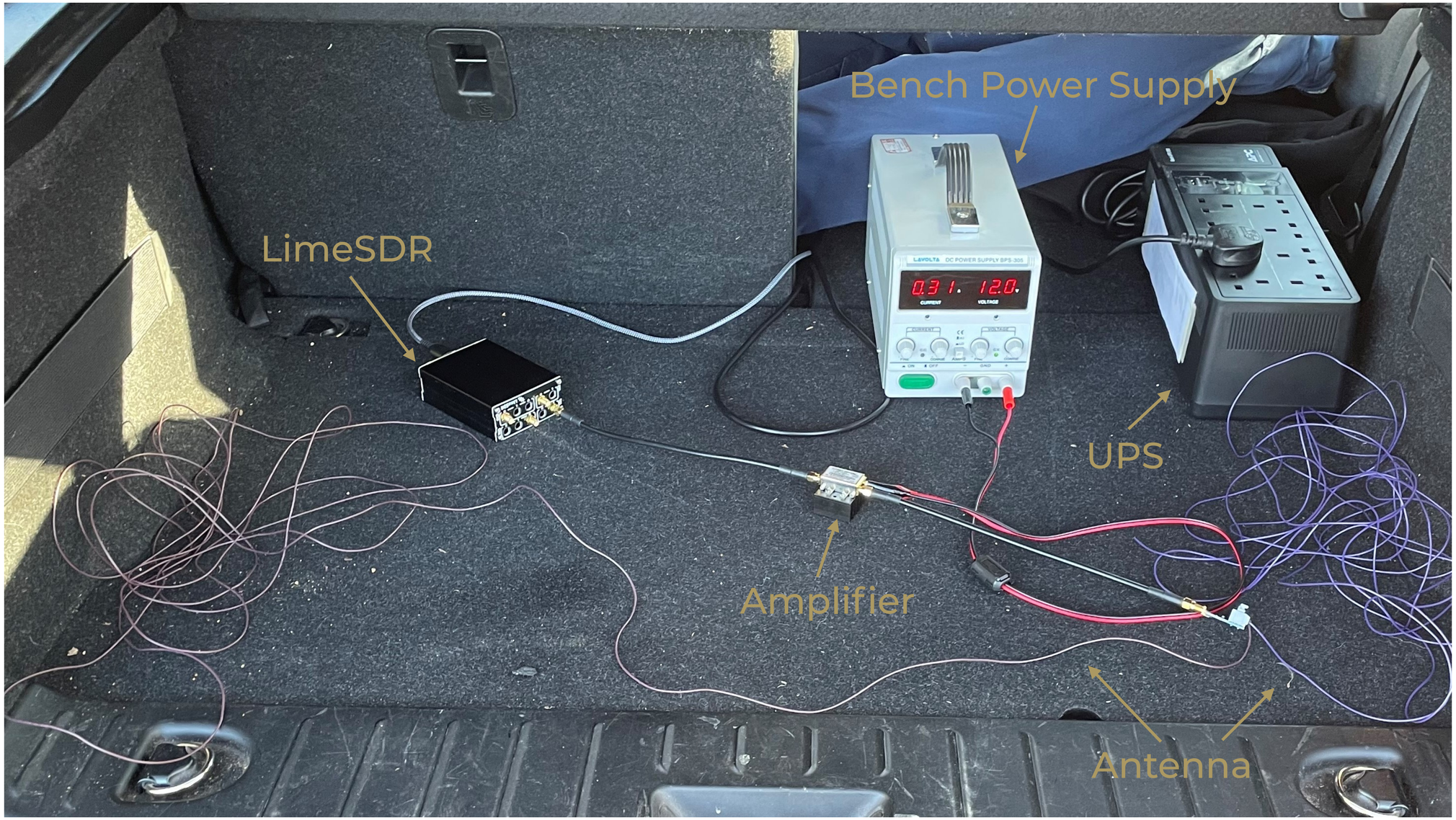




Lab Testing: Takeaways

- Getting access to specialized equipment can be difficult.
- Uncontrollable environmental factors might influence the results.
- Transmission power of a software-defined radio (LimeSDR) can differ between laptops.
- The software stack is crucial and different drivers might cause different results.
- Experiments involving PLC should be isolated from mains and preferably powered via batteries.

Real-World Testing: Equipment



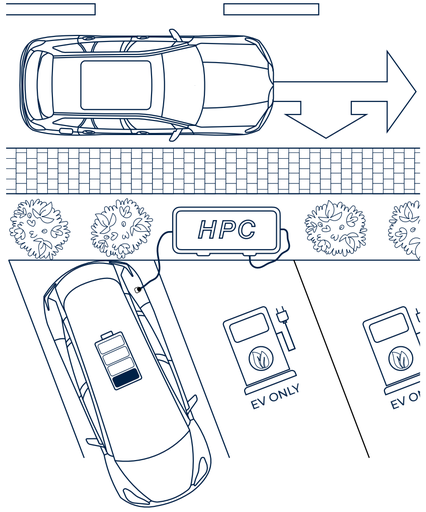
Real-World Testing: Method

- Charging station and vehicle are black boxes that do not provide any feedback.
- We followed a similar method as used in the lab experiments.
- We slowly increased the transmission power, until the charging stopped.
- We evaluated the same vehicle on multiple chargers and with different state of charge.
- We conducted the experiment for different settings, e.g., distances, angles and antenna alignments.
- Again, we repeated the experiments multiple times to ensure that uncontrollable environmental factors are taken into account.

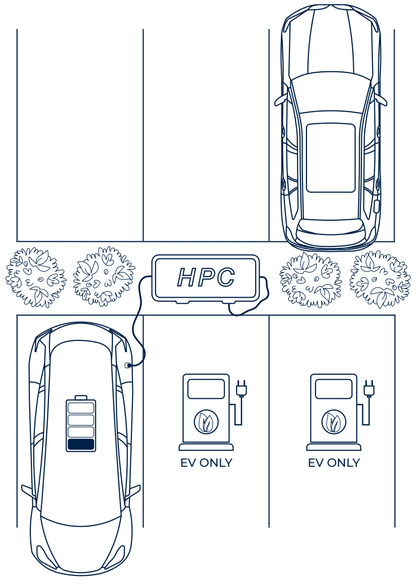
Real-World Testing: Vehicle Overview

Vehicle	Class	Price ($)	Charging Capacity
A	Subcompact	50,000	50 kW
B	Compact SUV	85,000	150 kW
C	Shooting Brake	150,000	270 kW
D	Subcompact	20,000	50 kW
E	Mid-size Sedan	50,000	120 kW
F	Mid-size SUV	70,000	150 kW
G	Compact	45,000	125 kW
H	Compact	32,000	50 kW

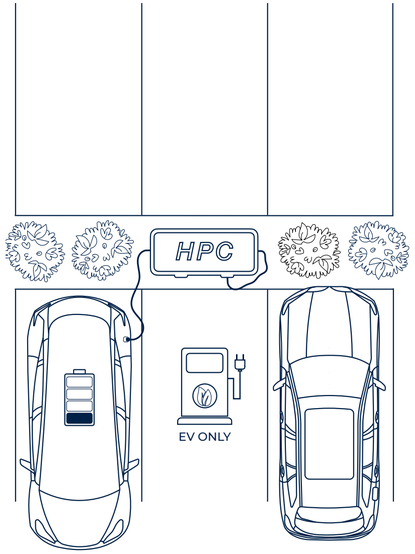
Real-World Testing



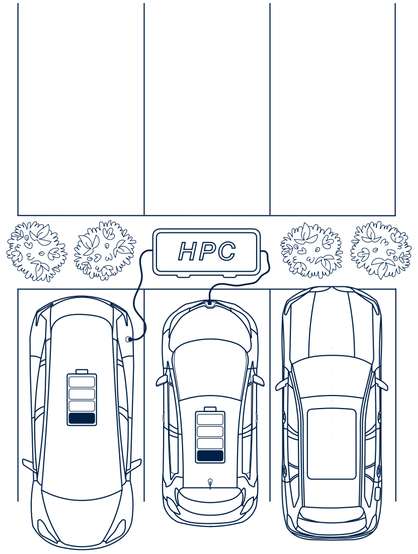
Scenario 1



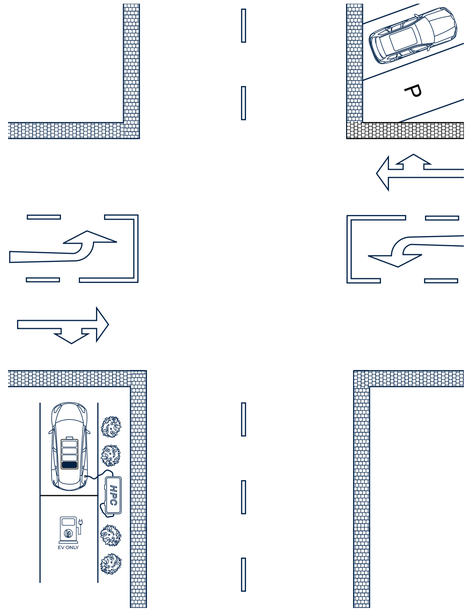
Scenario 2



Scenario 3



Scenario 4



Scenario 5

Real-World Testing: Challenges

- Experiments in a real-world environment involving the emission of electromagnetic waves must be carefully planned.
  - Is it possible to transmit at this frequency?
  - Are there any other communications in this spectrum? -> Check the government regulations.

- To help to ensure that the experiments meet all the requirements, project partners are important.
  - Due to the sensitivity of the topic, this can be challenging.

- It is crucial that the experiments do not affect anyone or anything else.
  - No other vehicles should be charging when running the experiment.

- Running the experiment in all possible settings is not possible.

- Keep the transmission time to a minimum.

Evaluating Wireless Attacks Against CCS Electric Vehicle Charging

- Did you use experimentation artifacts borrowed from the community?
- Did you attempt to replicate or reproduce results of earlier research as part of your work?
- What can be learned from your methodology and your experience using your methodology?
- What did you try that did not succeed before getting to the results you presented?
- Did you produce any intermediate results including possible unsuccessful tests or experiments?

Questions?

info@brokenwire.fail or sebastian.kohler@cs.ox.ac.uk

https://brokenwire.fail

https://github.com/ssloxford/brokenwire

https://nvd.nist.gov/vuln/detail/CVE-2022-0878