Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging

Richard Baker and Ivan Martinovic, *University of Oxford*

https://www.usenix.org/conference/usenixsecurity19/presentation/baker

This paper is included in the Proceedings of the 28th USENIX Security Symposium.

August 14–16, 2019 • Santa Clara, CA, USA

978-1-939133-06-9

Open access to the Proceedings of the 28th USENIX Security Symposium is sponsored by USENIX.

Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging

Richard Baker
University of Oxford
richard.baker@cs.ox.ac.uk

Ivan Martinovic
University of Oxford
ivan.martinovic@cs.ox.ac.uk

Abstract

Electric vehicles (EVs) are proliferating quickly, along with the charging infrastructure for them. A new generation of charger technologies is emerging, handling more sensitive data and undertaking more complex interactions, while using the charging cable as the communication channel. This channel is used not only for charging control, but will soon handle billing, vehicle-to-grid operation, internet access and provide a platform for third-party apps — all with a public interface to the world.

We highlight the threat posed by wireless attacks on the physical-layer of the Combined Charging System (CCS), a major standard for EV charging that is deployed in many thousands of locations worldwide and used by seven of the ten largest auto manufacturers globally. We show that design choices in the use of power-line communication (PLC) make the system particularly prone to popular electromagnetic side-channel attacks. We implement the first wireless eavesdropping tool for PLC networks and use it to observe the ISO 15118 network implementation underlying CCS, in a measurement campaign of 54 real charging sessions, using modern electric vehicles and state-of-the-art CCS chargers. We find that the unintentional wireless channel is sufficient to recover messages in the vast majority of cases, with traffic intercepted from an adjacent parking bay showing 91.8% of messages validating their CRC32 checksum.

By examining the recovered traffic, we further find a host of privacy and security issues in existing charging infrastructure including plaintext MAC-layer traffic recovery, widespread absence of TLS in public locations and leakage of private information, including long-term unique identifiers. Of particular concern, elements of the recovered data are being used to authorise billing in existing charging implementations.

We discuss the implications of pervasive susceptibility to known electromagnetic eavesdropping techniques, extract lessons learnt for future development and propose specific improvements to mitigate the problems in existing chargers.

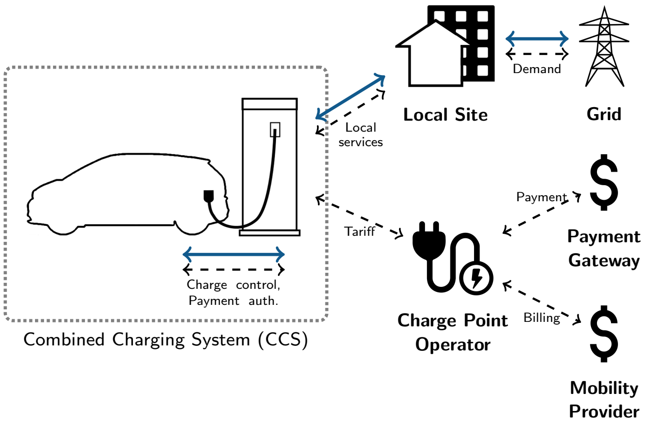


Figure 1: Overview of EV charging with V2G and payment options shown. Solid, blue lines indicate power flow whilst dashed, black lines indicate communication.

1 Introduction

The rise of electric vehicles (EVs) as a contemporary and future transport mechanism has been swift in recent years and continues to accelerate, helped by prevailing attitudes, technological advances and notable personalities contributing in the area. There are already widespread government plans to eradicate fossil-fuel vehicles in cities [61], states [28] and countries [9] in the coming years.

As EV technology advances rapidly, the availability of charging infrastructure has become a challenge for users, who require access both to private charging points at home and public ones on longer journeys. The lack of sufficient charging points is noted as a slowing influence on adoption of electric mobility [62] and this has prompted endeavours to expand the infrastructure, both from governments recognising the potential public good and from competing EV manufacturers who understand that having the best infrastructure makes their vehicles more appealing to purchasers. There are already multi-billion dollar pulibc deployment plans in progress [18] and predictions of worldwide numbers exceed 50 million chargers by 2025 if private systems are included [2].

With several major charging standards in existence, the race to become the dominant one has reached a fervour in recent years and a new generation of high-power charging systems has emerged. But the pressure to achieve rapid expansion has so often been seen to inhibit secure implementation. Users demand charging systems that are consistent and convenient, but with such drive for the adoption of electric mobility, it is critical that they are also secure. The security community has raised concerns in the past that standards do not fully address security and privacy issues [4, 8, 72], as well as noting vulnerabilities in back-end and payment systems of earlier charging system deployments [35, 19].

Meanwhile the complexity of developing all the infrastructure required for a secured charging network is enormous. As Figure 1 shows, vehicle charging involves interaction between the vehicle, the owner, the charger operator, a payment gateway and the grid regulator. This requires establishing communication links capable of supporting the higher-level protocols for this interaction, within a dynamic and untrusted environment, where many thousands of users come and go. It also necessitates trust relationships between all the participants to ensure each is acting legitimately.

In light of the challenges this infrastructure development faces and the acknowledged side-channel vulnerabilities that exposed cabling presents, we undertook to investigate the security of the charging cable communication.

We make the following specific contributions:

1. *Demonstrate that the use of powerline communication, and its specific configuration in CCS, makes systems particularly vulnerable to EM eavesdropping*
2. *Develop an eavesdropping system for HomePlug GP and the ISO15118 PHY-layer*
3. *Conduct a real-world measurement campaign, demonstrating the widespread nature of the problem*
4. *Highlight the potential for privacy violation and user tracking with existing systems*
5. *Propose countermeasures to mitigate the capabilities of an eavesdropper*

Our findings are relevant to thousands of chargers across Europe and North America [29, 67], along with having implications for ongoing deployments both in public locations and private homes.

2 Background

The availability of EV charging infrastructure is growing enormously. Early, simple alternating-current chargers are being superseded by a new generation of charging technologies that provide greater charging power and advanced functionality. The greater power is provided by the use of direct-current (DC) charging, allowing an enormous increase in current delivery over previous alternating-current designs. Public DC charging stations currently well exceed the 3kW power levels commonly available in a home, with 50kW supplies plentiful and those providing up to 350kW soon to appear [30][38]. But the improvements in *power* are only part of the benefit of this new generation of technologies. The *communication* capabilities are also vital to enable a host of new uses:

Reactive charging allows a vehicle to vary its charging process based on electricity price or expected time of departure.

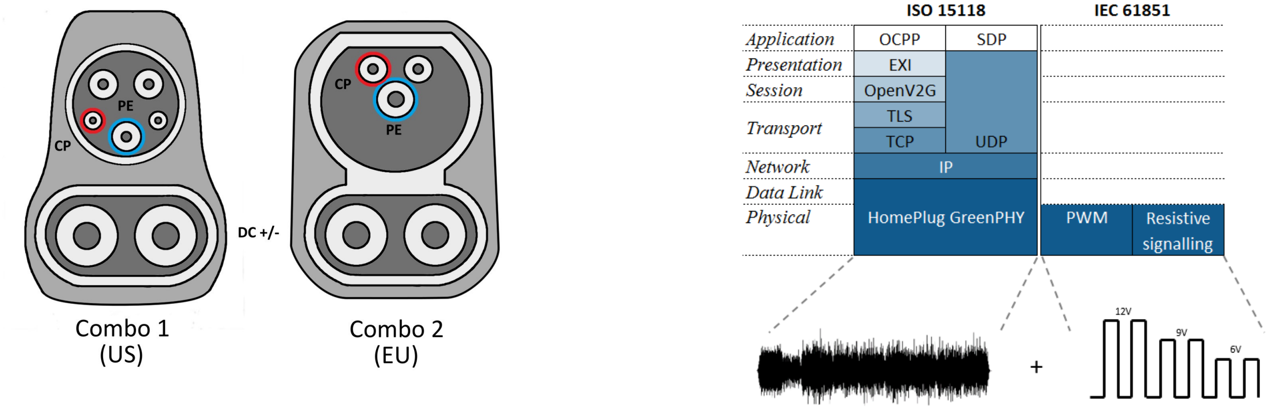
Automatic billing or “plug-and-charge” allows a vehicle to authorise billing of its owner for charging, without the owner explicitly interacting with it. Aside from the obvious convenience benefit, the same capability also allows the user to ‘roam’ between charging providers with a seamless experience as cross-provider billing is handled automatically as well.

Vehicle-to-Grid (V2G) makes use of bidirectional power flow to allow the vehicle to deliver energy as well as consume it. As energy prices fluctuate with demand, the vehicle can either act as a storage battery for a user’s home or sell energy back to the grid on demand. This can bring economic benefits for the user and stability improvement for the grid operator.

External payment is commonly provided by RFID cards [19], apps that communicate with the charger separately or card payment terminals. Additional systems exist though, for payment through separate providers or via a blockchain network [64, 74, 6, 26].

Additional services that operate in conjunction with charging are proposed [47]. In a private environment this might comprise access to the local network to communicate with smart-home devices or make use of domestic internet service and avoid mobile network charges. At public charging stations site-specific services such as loyalty schemes, to-vehicle delivery, parking charges or ‘where-have-I-parked’ reminders can operate, with middleware layers to support an app ecosystem in commercial development [22]. Internet access can also be made available for connected vehicles in areas without mobile network coverage, such as underground parking complexes.

Examples of each are in production use and deployment is



(a) Two charging cables are used by CCS. The Combo 1 and Combo 2 plugs are dominant in the US and Europe respectively, while other locations adopt one or the other. DC power is delivered by the large conductors at the bottom of the plug, meanwhile communication happens over the Control Pilot and Protective Earth lines (red and blue, respectively).

(b) CCS high-level and low-level signalling share the same communication lines. The corresponding ISO 15118 PLC and IEC 61851 systems have their signals superposed at the physical layer. The PLC provides a standard IP stack for use by charging traffic and other services.

Figure 2: Illustrations of the physical connectors for CCS charging, along with the network stack used for communication.

becoming more widespread. The underpinning communication mechanisms go beyond indicating presence and readiness to charge, also providing a general-purpose channel for software operating in the vehicle and charger. Figure 1 shows the potential extent of communication during charging. The vehicle can demand current flow, the charger can provide tariff information for reactive charging or reverse current demands for vehicle-to-grid, and the two can interact with external parties for automatic billing or to provide additional services.

Four major next-generation charging systems exist: CHAdeMO[1], Supercharger[2], GB/T 20234[3] and the Combined Charging System (CCS)[4]. Each uses the charging cable for primary communication: CHAdeMO, Supercharger and GB/T 20234 make use of CAN-Bus, whilst CCS makes use of powerline communication (PLC).

We examine the CCS standard as it has the most extensive, current functionality (supporting reactive charging, automatic billing and additional services) and has been adopted by seven out of the ten largest automobile manufacturers by production numbers [57]. In addition it is being integrated by competing manufacturers, such as Tesla [42].

2.1 Combined Charging System (CCS)

The Combined Charging System (CCS) is an amalgamation of standards governing all physical and logical elements of the charging infrastructure; from the physical connector to the protocols for automated billing. Figure 2a shows the charging plug, while Figure 2b illustrates the communications undertaken. The communication between vehicle and charger is standardised as ISO 15118. This uses powerline communication (PLC) over the Control Pilot (CP) and Protective Earth (PE) lines of the charging cable. The PLC shares the lines with the older IEC 61851 signalling system for backwards-compatibility reasons, with the signals superposed at the physical layer. The specific PLC implementation is HomePlug GreenPHY (HPGP) [5], a derivative of the commonplace broadband LAN technologies sold to consumers, that has been modified to support pairing between devices with no pre-shared key, and to be more robust to noise. Atop the PLC, ISO 15118 communication provides a full IP stack to act as the general-purpose channel. The same standard also defines interactions for identification, authorisation, tariff provision and control. Communication persists throughout the duration of charging and allows charge parameters to be varied quickly.

CCS provides reactive charging by allowing a charger to present current and future tariff information to the vehicle, which can then make charging requests based on a user's settings. The user may have a price preference or timing constraints for when the vehicle should be charged. Contract-based automated billing is implemented by having a user's contract with a charging provider represented by a public-key certificate stored on the vehicle. A complex public-key infrastructure (PKI) then allows the vehicle to authenticate the charger, the charger to validate the charging contract and the provider to produce verifiable metering receipts. The same PKI is used to underpin the TLS tunnel for protecting traffic.

[1] An open standard developed by Nissan and dominant in Japan

[2] A proprietary standard developed by Tesla Motors

[3] A nationwide standard in China

[4] An open standard backed by the European Union

Competing automated billing approaches do exist however, that do not use the contract-based approach, nor rely on the PKI. Blockchain-based payment systems, seeking to protect the user's privacy from charging operators, simply use the communication channel as a building block for their own service [6, 26]. A system named "AutoCharge" [58] is also used in some networks [33, 56] to enable automated billing for even those users whose vehicles do not support the required certificates. The AutoCharge system is based on a simplified ISO 15118 use-case [52] that uses only vehicle-provided identifiers to match the vehicle to a customer record at the provider.

As there is a general-purpose channel, any IP communication is supported for additional functionality. Fast internet access is suggested in the ISO 15118 standard and a selection of data collection, targeted marketing, on-demand entertainment and third-party app platforms are emerging to take advantage of this [6, 22].

2.2 CCS Security

Communication security is considered in many of the systems making up CCS standard; with traffic encryption available at the PHY layer, TLS at the Transport layer and XML Security at the Application layer [55, 48].

At the PHY layer, the HPGP PLC network maintains a shared secret key called the Network Membership Key (NMK), with ephemeral Network Encryption Keys (NEKs) rotated periodically. All MAC-layer traffic is encrypted via AES-128 using the NEK. However, HPGP security is based upon a private-network model, while EV charging is fundamentally a public-network model. To adapt the technology to the use case, additions were made to HPGP to incorporate an initial association protocol[5], during which the vehicle and charger verify that they are connected to each other and are not communicating with the wrong party due to crosstalk on their communication cable. The determination is known as Signal-Level Attenuation Characterisation (SLAC) and is illustrated in Figure 3. The protocol involves the vehicle sending a series of sounding messages, for which the charger reports the measured attenuation. If multiple chargers respond due to crosstalk, the one reporting the least attenuation is selected and communication commences. Once a charger is selected, a Network Membership Key is created by the charger and used to establish a private network. The key is then sent to the vehicle in the final `CM_SLAC_MATCH.CNF` message of the protocol. The SLAC protocol can operate in a secure mode, with mutual authentication and encrypted communication, but this capability is optional if supported by both parties. Indeed, despite the availability of this mechanism, the ISO 15118 standard specifies that SLAC only operates in its plaintext mode, leaving message security to TLS.

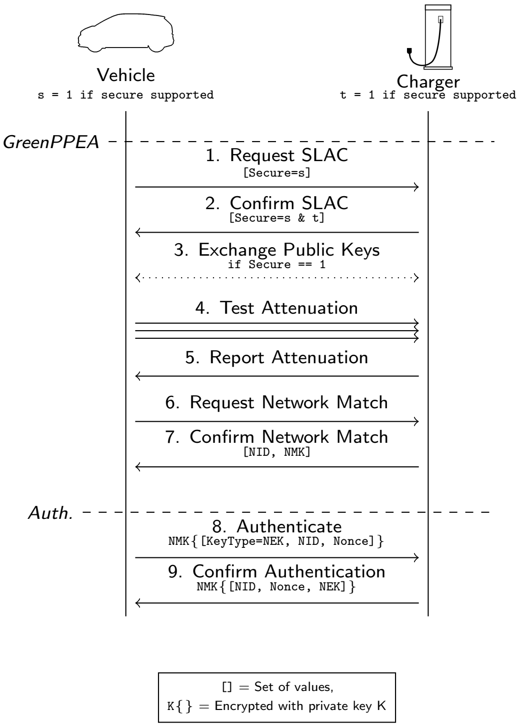


Figure 3: An overview of vehicle-to-charger network establishment in HomePlug GreenPHY. If the secure mode is supported by both parties and enabled in initialisation then step 3 occurs, allowing the messages in steps 5–7 to be signed and the one in step 7 also encrypted.

Once a network is established, a TLS connection is only created under certain conditions. If contract-based automated billing is used then TLS is required, similarly for the discovery of additional services, but only when they are ones defined in the ISO 15118 use cases. When charging is externally authorised, no TLS is required for the control traffic [48]. The options for external authorisation are open; including RFID cards, mobile-app networks, manual authorisation by a charger operator or some other service operating on the charger. The method need not be external to the charger, only external to the ISO 15118 scope. For all other traffic not managed through a standard use case, security is left to the implementer. In the alternative payment example of [26], independent IP communication is undertaken completely outside the scope of ISO 15118 (although secured in an SSH tunnel in that case).

3 Related Work

The privacy and security issues surrounding EV charging are the subject of ongoing work; with attempts to devise architectures that protect each stakeholder [32, 40] and analyses of the security of upcoming standards [4, 10, 8]. These works

[5] The comprehensively-named GreenPPEA, or "GreenPHY Plug-in-electric-vehicle Electric-vehicle-supply-equipment Association"

are theoretical in nature, however, and leave aside implementation issues. They also assume a wireline threat model for attacks on the vehicle-to-charger communication, discussing where an attacker must use “a modified cable or an adapter plug installed on the [charger]” [8]. By contrast, we consider a wireless threat model that permits deniability on the part of the attacker.

Practical attacks have been demonstrated on previous-generation infrastructure, particularly against RFID authorisation [35, 19], but require the attacker to clone a user’s physical token or access debug ports on an unlocked charger.

Since electromagnetic emissions security was brought from a military discipline into academic study by van Eck’s work on eavesdropping video displays [68], efforts have been devoted to studying a wide range of systems [7]. Recent work has focused primarily on extracting secrets from operating devices [3, 13], although the emissions security of digital communication systems have been studied in the context of eavesdropping on RS232 serial devices [66] and 100BaseT ethernet [63], along with use as a covert channel for USB [39]. While radiated emissions from powerline communication have been studied from an electromagnetic compatibility perspective [71], we demonstrate the first practical wiretap attack using these emissions.

Vehicle tracking using unique identifiers has been studied in the context of electronic license plates [41], tire-pressure monitoring systems [46] and vehicular ad-hoc networks [49], highlighting the impact upon individuals’ location privacy and inspiring this work on new charging technologies. Practical attacks have also been demonstrated to wirelessly compromise in-vehicle systems [17], to unlock vehicles for theft via remote keys [70] or passive entry [34, 37] and to misdirect drivers to unwanted locations [73]. These attacks consider an active attacker with different goals to those studied here and as such could be considered orthogonal to our work.

Energy monitoring has been shown to enable the tracking of individuals [54] and this has prompted proposals to mask energy signatures, such as by using rechargeable vehicle batteries [69], which assumes that data about vehicle power flow cannot be monitored.

4 A Near-Ideal Side-Channel

The underlying principles of electromagnetic (EM) side-channels are very well-explored and their study has informed modern security design [7]. Despite this, we describe here how the use of PLC and its specific arrangement within CCS exacerbates the vulnerability to EM attacks.

The design of PLC technologies assumes differential signalling; wherein two identical transmission lines that are located in close proximity are driven with equal but opposite signals, such that those fields largely cancel and no residual electric field exists. Practical challenges often break these underlying assumptions for in-home PLC deployments, leading to EM interference and susceptibility thereto [71]. Despite EV charging requiring simpler and more constrained wiring than domestic electrics, these assumptions are still broken in CCS. A design choice to incorporate backwards compatibility with an earlier low-power charging standard led to a PLC circuit design that connects one transmission line to ground (see Fig. 2b and App. A). This renders the signalling *single-ended instead of differential*. With no inverse field, the charging circuit functions as a suitable antenna for emissions or interference.

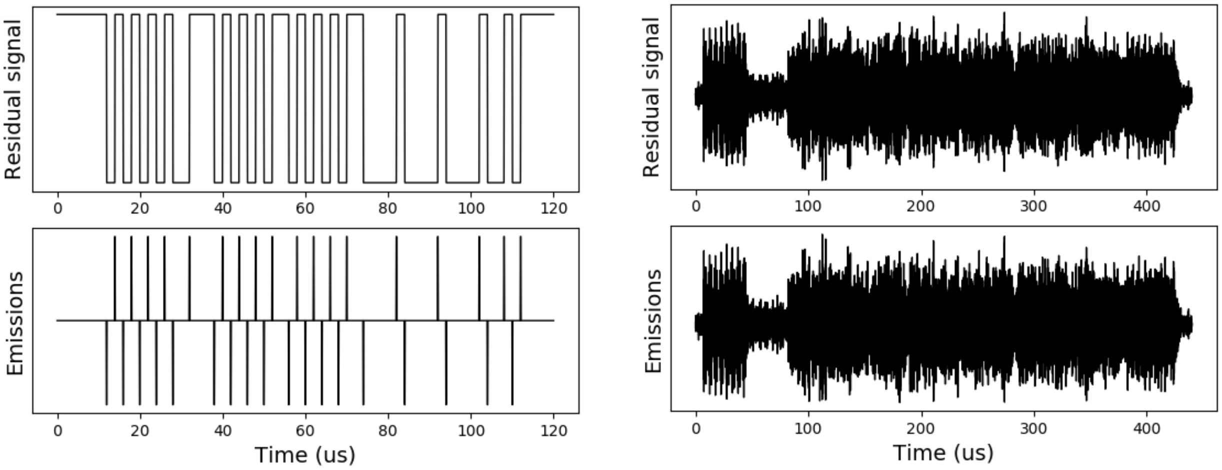
The nature of the PLC waveform itself, however, makes it ideal for wireless observation and interaction. It can be seen in Figure 4, operating as a single-ended system alongside single-ended CAN-Bus communications for comparison. The radiated signal represents the gradient of the original signal: only the changes in voltage. This introduces a minor problem for an attacker whenever they wish to observe and a major one when they wish to inject signals with constant voltage levels, most notably the square waves used ubiquitously in digital communication (and in other EV charging communication based on CAN-Bus). In observation the static voltage produces no response, so only state transitions are detectable. The attacker uses these where they can or hopes for the signal to leak elsewhere in the circuit and be modulated onto a more easily-observable one [7]. In injection the attacker cannot directly induce the desired static voltage level and instead must exploit nonlinearities in components or undersampling effects in order to synthesize the signal at the victim [51]. The absence of components to subvert, or the presence of filtering in the target circuit, limit the attacker’s opportunities.

Broadband PLC technologies predominantly use orthogonal frequency division multiplexing (OFDM); in which the data are modulated in the frequency domain before constructing a time-domain waveform using an inverse Fourier transform. The resulting, transmitted waveform is a finite sum of sinusoids and does not exhibit any non-zero static voltage levels. *The observed emissions simply form a phase-shifted replica of the original signal.* The attacker therefore does not need to make inferences to determine the original signal from eavesdropped observations, nor predict what transformations an injected signal will undergo in the receiver. They need only contend with the characteristics of the channel itself.

5 Threat Model

While we discuss the channel properties in a bidirectional sense above, we focus our further investigation and practical attacks on passive eavesdropping. Testing on deployed infrastructure restricts us to only passive operation.

The attacker listens to the unintended electromagnetic radiation of the EV charging communication. Their goal is to eavesdrop on the general-purpose channel established be-



(a) CAN-Bus.

(b) PLC.

Figure 4: Example single-ended signals, with the radiated emissions that result. As the emissions are the gradient of the signal, the square wave produces only impulses while the OFDM waveform is all but unchanged.

tween the vehicle and the charger; such that they obtain access to private data it carries. The attacker can approach close to the target vehicle and charger but cannot modify or interfere with the equipment. They perform their attack either *in-person* from a nearby location, or by *situating a device* at the site and leaving it unattended.

We justify this model on the basis of deniability and access. Interfering with a vehicle or charger is an immediately suspicious activity that would draw attention from the owner, people nearby and operators reviewing CCTV footage. The charging equipment is also handled regularly by drivers, so a cable modification or plug insert is more likely to be noticed. By contrast parking near another vehicle at a public station or briefly visiting a private property appear to be benign actions.

6 PLC Eavesdropping Tool

Given the properties described in Section 4, the passive attacker's task is the same as that of a legitimate receiver; to maximise the signal-to-noise ratio (SNR) and bandwidth (BW) of the received signal. In a real setting, additional complicating factors exist. While the exposed components are the most obvious targets, any element of the communication circuit (i.e., charging plug, cabling, vehicle, charger), or indeed multiple elements, could act as an unintentional antenna(s). The size of the equipment makes potential antennas physically distant from one another, so it can be difficult to predict the location that optimises the SNR and BW for each target. Similarly, electric vehicles and chargers are powerful electrical devices and even minor imperfections can introduce significant interference levels, which must be suitably mitigated by careful positioning or filtering.

Exploiting the properties and design choices of CCS, we developed a tool for wireless eavesdropping of the underlying physical layer; a HomePlug GreenPHY (HPGP) network. The tool is applicable to monitoring any HPGP network as well as network management traffic in HomePlug AV and AV2 networks, although the vehicle charging scenario is particularly beneficial for the reasons discussed above. The tool is available open-sourced under the MIT licence[6].

The eavesdropping tool broadly resembles a normal HPGP receiver. While the HPGP standard is public, all compatible implementations are proprietary and implemented as integrated circuits. Our pure-software implementation allowed far greater insight and flexibility during captures however, particularly for experimenting with different preprocessing steps to improve reception and collecting partial data that would be discarded by a black-box implementation. The receiver architecture can be seen in Figure 5. Given that Wi-Fi shares the same OFDM underpinnings, the overall structure bears many similarities to a Wi-Fi receiver, albeit distinct in details to match the HPGP protocol specification.

As the signal processing chain is complicated we describe it briefly here but elide full details from the main text, providing them in Appendix B instead. The signal is captured and digitally filtered to suppress local interference. Messages, known as PHY-layer Protocol Data Units (PPDUs), are identified using a power detector and correlation of the signal preamble against the known preamble structure. As an OFDM technology, data are represented in individual *symbols* throughout the Frame Control and Payload sections of

[6] https://gitlab.com/rbaker/hpgp-emis-rx

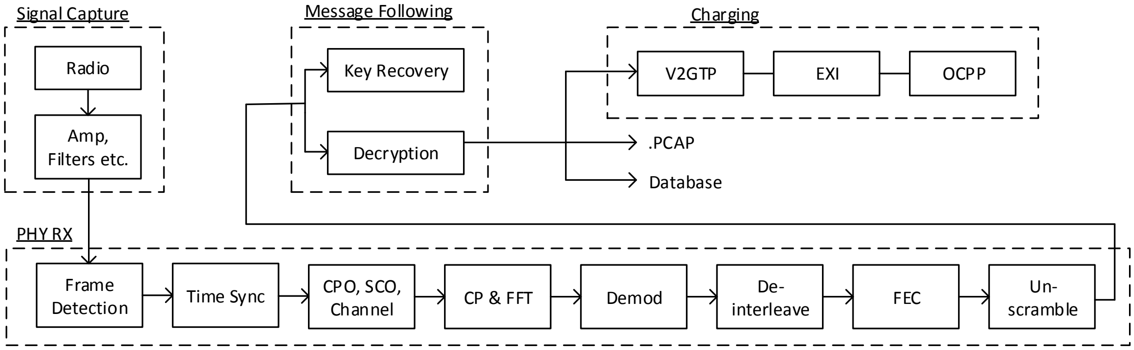


Figure 5: Architecture of PLC monitoring tool. The signal is captured and prefiltered, before moving through a software receiver chain to recover messages. The message following behaviour extracts security-relevant data and stores all messages. Charging traffic can be further processed, while traffic using other protocols will need separate onwards processing.

the PPDU. Once the receiver is time synchronised to the PPDU, each symbol is processed in turn; with channel estimation and frequency offset correction applied before demodulation. With complete messages the Turbo Code error correction is processed to reduce errors and the Cyclic-Redundancy Check checksums are calculated (a CRC24 for the Frame Control and a CRC32 for the Payload). The application of the Turbo Code decoder is limited in our tool, owing primarily to the computational cost of the process. A Turbo Code is intended to be decoded by iterating a probabilisitic decoder over various rearrangements of the received bits. We use only a single pass of the decoder and its application already dominates the message reception time; exceeding the rest of the software processing chain. As such we suffer from reduced error-correction performance compared with an arrangement using multiple repetitions. Such an arrangement could be expected to receive more messages correctly in all circumstances.

7 Real-World Measurement Campaign

To explore the accessibility of the wireless side channel, we undertook a data collection campaign with three fully-electric vehicles: a BMW i3, a Jaguar I-PACE and a Volkswagen e-Golf. The campaign comprised over 800 miles of driving and spanned six major administrative regions of the UK. A total of 54 unique charging sessions were conducted, at locations including service stations, highway rest stops, superstores and hotels.

During charging sessions, we monitored radiated emissions to measure the extent of signal leakage and the ability of an attacker to eavesdrop it. Where we were able to receive sufficient emissions we used the tool detailed in Section 6 to recover the original transmissions and examine the communication itself. For the majority of our testing we monitored

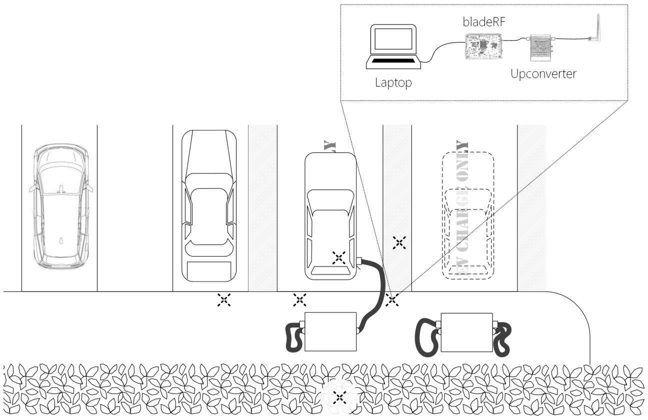


Figure 6: A composite diagram showing the experiment layout. The five antenna locations are denoted with a dashed × symbol.

one vehicle at a time, although we did conduct testing with multiple vehicles to examine the effects of cross-traffic. Further details of the locations and installed hardware are given in Table 1, while examples can be seen in Figures 7 and 8. All of the chargers are state-of-the-art at the time of writing. We tested only public chargers due to their availability, but equivalent chargers for private use are also on sale [25]. As the chargers were public, we did not modify or interfere with the equipment in any way. The vehicle, charger and associated cabling remained entirely untouched. While this prevented us from injecting messages or capturing ground-truth via a directly-connected receiver, it was necessary to conduct a widespread survey of existing infrastructure.

At each site, the vehicle was parked and connected to the charger for a series of charging sessions[7]. The receiving an-

[7] Care was taken to ensure we only observed signals from our own vehi-

				Vehicle			
Site	**Location**	**Type**	**Charger (Operator)**	**i3**	**I-PACE**	**e-Golf**	**Charge Sessions**
A	Oxford Belfry, Oxon.	Hotel	DBT Dual DC [20] (Polar [14])	✓			1
B	Abingdon, Oxon.	Superstore	DBT Dual DC [20] (Polar [14])	✓			1
C	Maldon, Essex	Superstore	ABB Terra 53 CJG [1] (POD Point Open [59])	✓			1
D	South Mimms, Herts.	Road services	DBT Dual DC [20] (Ecotricity [23])	✓			1
E	Bishops Stortford, Herts.	Road services	DBT Dual DC [20] (Ecotricity [23])	✓			1
F	Hythe, Kent	Road services	DBT Dual DC [20] (Ecotricity [23])	✓	✓	✓	9
G	Dover, Kent	Superstore	ABB Terra 53 CJG [1] (POD Point Open [59])	✓			10
H	Marden, Kent	Local garage	Chargepoint CPE200 [43] (InstaVolt [44])	✓	✓	✓	15
I	Chatham, Kent	Racetrack	Chargemaster Ultracharge 500S [12] (Polar [14])			✓	1
J	Ticehurst, Kent	Golf club	Chargemaster Ultracharge 500S [12] (Polar [14])		✓	✓	4
K	Hawkhurst, Kent	Local garage	EVTronic QUICKCHARGER [31] (GeniePoint [15])		✓		2
L	Tunbridge Wells, Kent	Local garage	Efacec QC45 [24] (Shell Recharge [65])			✓	2
M	Hastings, Sussex	Local garage	EVTronic QUICKCHARGER [31] (GeniePoint [15])			✓	1
N	Milton Keynes, Bucks.	Public car park	Efacec QC45 [24] (Polar [14])			✓	5

Table 1: Details of all tested charging locations, across the southern United Kingdom. There were a total of 54 unique charging sessions. Multiple signal captures were taken during each session; at initialisation, during charging and at shutdown. At sites **F** and **H**, two vehicles were charged and monitored simultaneously.

tenna was placed at various locations to investigate the reception capabilities. As noted in Section 6, deriving an optimal attack location beforehand is challenging, so this placement was exploratory. The locations are illustrated with a dashed × symbol in Figure 6. Locations near the cable itself, on the outside of the vehicle, within the vehicle, hidden in a nearby hedge and on a nearby car were all tested. As each site had a different layout, Figure 6 is a composite to show the arrangements, rather than a meticulous depiction of any one site.

The data were collected using a bladeRF software-defined radio, an RF Explorer Upconverter and a GNU Radio flowgraph running on a Lenovo Thinkpad X1 Carbon laptop. We made use of an electrically-short monopole antenna to collect the signal. Owing to the long wavelengths involved, testing with a suitably-tuned directed antenna was not possible. The equipment for our experiments cost approximately $800, although equivalent setups are available for less than $300. The collected signal was passed through 25dB amplification and upconversion (+530MHz) to bring it into the tunable range of the bladeRF. Initial filtering and packet detection was performed with further GNURadio flowgraphs, while subsequent processing was implemented using Python and numPy libraries. We tuned the receiver's interference-rejection filter by observation at each site, but left all other reception parameters constant throughout.

8 Results

In this section we examine the results of our testing in real environments, both in terms of raw observable signal and message recovery.

8.1 Eavesdropped Communications

Table 2 details the observations for each site. It indicates the peak signal-to-noise ratio (SNR) over all the sessions, along with the widest bandwidth (BW) with a positive SNR. It then lists the count of all PPDUs detected, the number of data PPDUs, the rate at which messages were well-formed and the rate at which messages had a correct CRC32 checksum.

Every site displayed some form of unintentional wireless channel from the PLC communication, with properties that exceeded our expectations. The weakest signal showed 9dB from the peak to the background and spanned a bandwidth of 4.5MHz. In the best case 25MHz could be seen, up to a peak of 35dB. This was true irrespective of charger manufacturer, indeed varying notably between sites with the same charger hardware antenna location. This would seem to confirm the expectation that the site layout and variations in parking have a substantial impact upon reception.

Figure 9 shows spectrograms of the captured signal at a selection of sites, covering each tested antenna location. Overlaid on each subfigure is the utilised HPGP spectrum, showing the regions of the band in which transmission occurs. A transmission will originally have a frequency-domain representation that matches the spectral mask, with a peak power of -50dBm in utilised regions. Apparent power levels up to approximately -70dBm we observed, although the receiver was not calibrated against a reference scale so this value is uncertain. The degradation of signal across the band is clear in every case; the flat-topped spectral usage of the transmission is observable as a jagged range with many subcarriers severely attenuated, particularly at lower frequencies. This correlates well with studies of the wireline channel that legitimate receivers (with a conductive connection) experience, albeit with a different noise profile [53].

cles. Upon arrival we waited for any other users to leave before capturing traffic and aborted immediately if another arrived.

Site	Antenna	Peak SNR	BW	Total	Data	Bi-direc.?	Start?	RX%	CRC32%		
		(dB)	(MHz)	PPDUs	PPDUs			Mean	Min	Mean	Max
A	In car	15	6	526	272	✓		99.3	1.1	1.8	3.3
B	In car	18	12	1063	567	✓		29.8	0.5	3.3	5.3
C	In car	25	14	2976	1819	✓		99.9	46.6	48.1	50.3
D	In car	10	12	556	293	✓		88.2	1.4	2.3	3.0
E	In car	9	4.5	569	306			100	11.0	11.1	11.2
F	In car	21	12	3660	2009	✓	✓	99.3	27.8	36.8	45.8
	Bay behind	15	8	1434	1430	✓		99.3	**43.5**	43.5	**43.5**
	Outside car	10	10	12987	8255	✓		76.2	34.9	46.6	89.5
	Two cars	14	11	2449	2274			99.1	**24.3**	47.5	70.8
G	In car	19	12	5837	3670	✓	✓	99.0	51.1	60.3	71.4
	Next bay	15	13	4157	2749	✓		99.7	**91.8**	91.8	**91.8**
	By cable	29	23	23984	17246	✓	✓	80.2	52.9	74.0	**99.8**
H	In car	16	12.5	15052	9362	✓		99.2	69.9	71.0	72.8
	Outside car	20	11	16243	10407	✓		99.5	27.7	61.6	**80.6**
	By cable	35	25	19535	14717	✓	✓	92.1	**34.2**	70.0	92.8
	Two cars	15	12	24121	21006			99.6	42.2	71.9	**94.8**
I	In car	20	12	1501	1193	✓	✓	98.0	94.8	97.4	**100.0**
J	In car	20	7	14231	10291	✓	✓	81.0	1.0	33.6	67.9
	Outside car	23	7	1084	935	✓	✓	96.0	49.2	49.2	49.2
K	In car	8	5	1971	1278	✓		92.5	**0.0**†	22.0	38.3
L	Outside car	8	7	3004	1849		✓	25.8	**0.0**	0.0	0.0
M	In car	20	12	13631	9743	✓	✓	98.8	42.4	64.9	82.5
N	In car	24	14	4317	3364	✓	✓	68.3	**0.0**†	44.5	72.6

Table 2: Eavesdropping results, from all sites and antenna locations. Raw signal properties are quantified as Peak SNR and Bandwidth. PPDU counts are given and the observance of bidirectional traffic and session startup is indicated. The rates of well-formed messages are then shown, along with the rates of CRC32 checksum validations. The worst and best performance for each antenna location is highlighted in **bold** († indicates joint-worst).

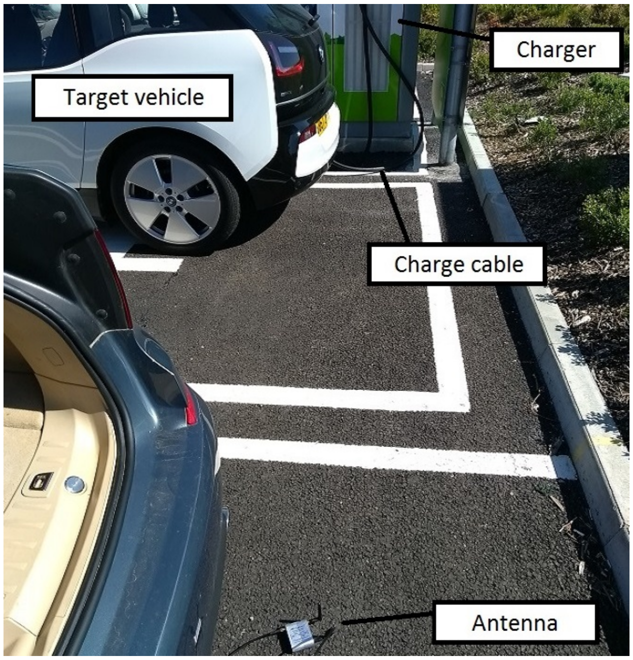


Figure 7: Eavesdropping from the next parking bay (site G), more than 4 metres away on the other side to the charging cable. In this arrangement 91.8% of messages were received successfully.

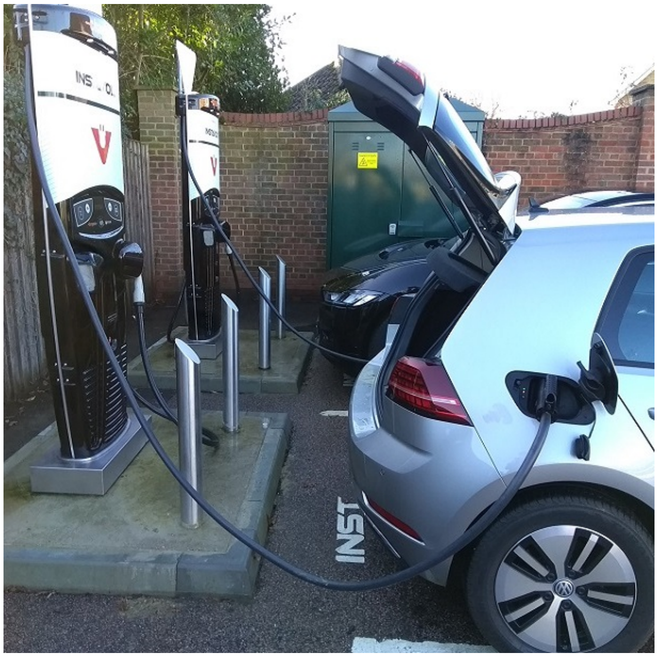
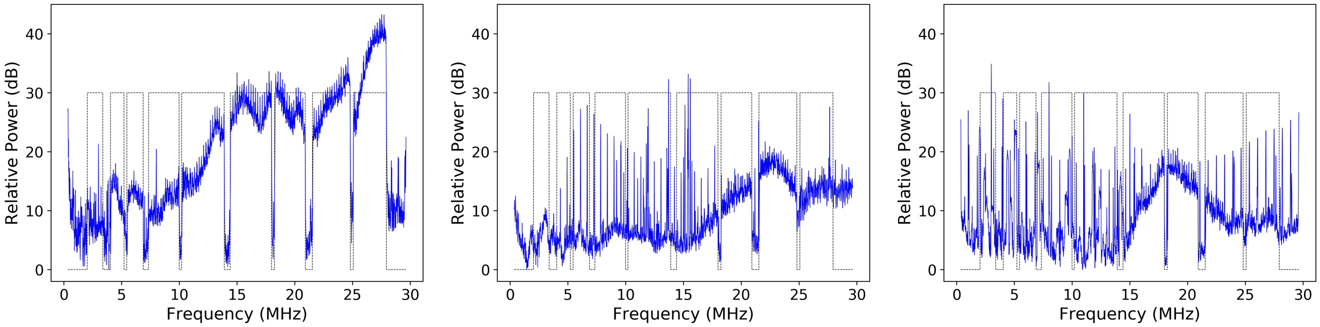


Figure 8: Two vehicles charging simultaneously. With the eavesdropper between the two vehicles 42.5% of messages were received successfully, including the NMK key establishment for both vehicles.



(a) Antenna by cable (site H)

(b) Antenna in bay behind (site F)

(c) Antenna in next bay (site G)

Figure 9: Observed signal across the HPGP bandwidth, at each antenna location. The HPGP spectral mask is overlaid to indicate the regions in which transmission occurs, although no valid comparison can be made with its power value as the measurement was not calibrated. Signal degradation and noise ingress is visible in every case, although far more prominently in (b) and (c).

8.2 Effects of Location

While systematic examination of performance by location was not our goal, we were able to observe trends across tested antenna positions, with the fidelity of the wireless channel varying substantially. The closest representation of the transmitted signal is that shown in Figure 9a, obtained approximately 0.5m from the charging cable. At other antenna positions the signal loss was more pronounced, both inside and outside of the vehicle, and in isolated cases the signal was swamped by interference more than a short distance from the cabling. Making general predictions about the channel gain at specific distances is not feasible due to the low frequencies at which the PLC operates (2 – 28MHz). Even at 28MHz the wavelength is still 10.7m and so all observations were taken well within the near field of the transmitter. In this region, common path loss calculations like the Friis equation [36] are not defined and near-field effects can change the channel gain drastically from position to position. Nevertheless, Figures 9b and 9c show the results of tests at the greatest distances; 4.2m in the latter case when the antenna was positioned by a vehicle in an adjacent parking bay (shown in Figure 7). Interference is still substantial at these distances (e.g., everything below 15MHz in Figs. 9b and 9c), but in the higher reaches of the band signal still easily visible.

The consistency of observed leakage across different charger hardware indicates that the issue is not isolated to a single implementation; supporting the claim that the design choices in CCS make a wireless side-channel for the PLC communication a systemic problem.

8.3 Message Recovery

With such a clear channel, message recovery proved highly successful, with hundreds of complete messages captured even in short sessions. In the best case, at site **I**, 100.0% of received messages had correct CRC32 checksums, more surprisingly 91.8% were still received when the antenna was located in the next parking bay. Reception rates were broadly correlated with raw SNR and BW, with improvements to either benefiting the performance. However this was not universal, as the very poor performance at sites **B** and **K** shows. Site **B** showed poor results despite far higher SNR and BW than Site **K**. Reception performance is broken down by location in Table 2, with the lowest minimum and highest maximum for each location highlighted in bold. Without ground-truth for the number of messages sent by each party, we cannot determine the number of messages missed entirely (only those received with errors), although the only unreported messages would be those that did not even trigger the packet detection algorithm (see Appendix B). Examining Frame Control headers showed that traffic was observed bidirectionally between vehicle and charger in all but two cases.

As charging stations, at least in public, are busy venues, we tested whether multiple simultaneous charging sessions caused interference that affected the wireless channel quality. Two vehicles (a Jaguar I-PACE and a VW e-Golf) charged simultaneously in 5 charging sessions at 2 locations, one of which is shown in Figure 8. In each case, one vehicle initiated charging first and then the second did so. The eavesdropper's antenna was located between the two vehicles and attempted to listen to both. In all cases, the eavesdropper was able to listen to traffic from both vehicles, albeit with varying success. At worst, 24.3% of messages were received with correct CRC32, at best 94.8% (mean 59.7%).

9 Security Analysis

In this section we analyse the captured communications and their security implications.

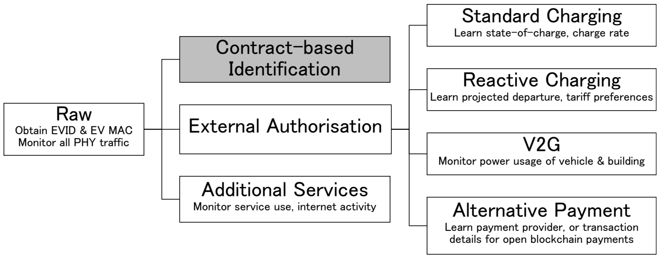

Raw
Obtain EVID & EV MAC
Monitor all PHY traffic
Contract-based Identification
External Authorisation
Additional Services
Monitor service use, internet activity
Standard Charging
Learn state-of-charge, charge rate
Reactive Charging
Learn projected departure, tariff preferences
V2G
Monitor power usage of vehicle & building
Alternative Payment
Learn payment provider, or transaction details for open blockchain payments

Figure 10: Tree diagram indicating the potential data available under a range of communication scenarios.

9.1 Unencrypted Communications

Where our testing campaign captured the initialisation of a charging session, we were able to examine the NMK exchange to form a network. In line with the ISO 15118 standard, every SLAC interaction we observed operated in insecure form. As such, the NMK was delivered in plaintext and the only barrier to acquiring it was receiving the message intact. We were able to intercept the `CM_SLAC_MATCH.CNF` message in 31 cases and acquire the NMK. Testing two vehicles side-by-side, in 4 sessions the attacker was able to extract an NMK value for one vehicle, meanwhile in one session both NMK values were extracted. In 9 cases, the subsequent `CM_GET_KEY.CNF` message was also recovered to obtain the ephemeral NEK and permit *passive decryption of physical-layer traffic*.

Examining compromised sessions, we saw the expected behaviour as the vehicle and charger established a network, the vehicle undertook the discovery protocol to find a charge controller and the two established a TCP connection. *No TLS tunnel was established in any charging session we observed*, leaving the high-level protocols exposed. Where external authorisation is employed, as it was in our testing, the use of TLS is optional under ISO 15118. Yet its complete absence from any vehicle or charger came as a surprise, especially given the charging locations were all public.

As a result we confirm that a passive attacker can wirelessly monitor all traffic at the PHY layer and that this ability *results from standards-compliant behaviour*, suggesting it is persistent. Likewise, the option to forego TLS means charging data is also left in the clear. We discuss this situation and its implications in Section 10.

9.2 Private Data

Figure 10 provides a breakdown of potential data available when eavesdropping, under various charging conditions or in the presence of different services. The PHY-layer traffic is always available and permits access to any higher-level communication, such as charging or internet access, that does not take additional steps to secure itself. Two unique identifiers for the vehicle are also available: its EV ID and its MAC address. These identifiers are persistent for the entire lifetime of the vehicle, including between owners, and are globally unique. They have been noted as personal data in previous privacy studies [40] and are covered by the European Union's GDPR as data that can be easily combined with other sources to identify an individual.

With contract-based billing, we do not expect charging traffic to be available, as TLS is always required in this case. However as we have seen, when it is optional to omit TLS, this has consistently been done. Currently, this leaves the majority of charging traffic in the clear at public locations, although these are likely to be the earliest adopters of contract-based billing (or some alternative). The long-term omission of TLS at private locations is of greater concern. Indeed it is in this case that there is more potential for behavioural profiling, due to the vehicle staying far longer at the user's home or workplace and with the emerging Reactive Charging and V2G systems far more beneficial to them there. The introduction of 'Vehicle-to-Home' capabilities, for instance, is prioritised for introduction as early as 2020 by the CCS standards body [16]. Resulting indicators of the user's day-to-day behaviour such as the vehicle's state-of-charge and projected departure time are contained within normal charging traffic, while reverse power flow data in a V2G system yields insights into the power usage of the building.

In addition to internet access for in-vehicle entertainment systems, third-party apps and alternative payment networks, the traffic of any local services would also be available at public locations, as would smart home integration traffic in private ones.

9.3 Charging Attacks

A reliable eavesdropping capability presents a range of opportunities for an attacker, both immediate and longer-term in their impact. We consider here a selection of potential attacks using these techniques. Although we did not perform the attacks against public chargers, we describe how they would be conducted.

AutoCharge Extant AutoCharge systems, such as one operating in production across a 60-location network in three European countries [33] are at particular risk from wireless eavesdropping. The use of the vehicle's charge-controller MAC address for billing identification [58, 56], while highly questionable from a purely-security standpoint, was undertaken for compatibility and convenience benefits (and has been lauded as such by customers). What may be an acceptable trade-off when physical interference is required to extract the values, is far less so when this can be done from another vehicle without any observable signs. The identifiers of the vehicles are shown partially-masked below (none is a customer of an AutoCharge system):

Vehicle	MAC
BMW i3	`f0:7f:0c:02:●●:●●`
VW e-Golf	`00:7d:fa:01:●●:●●`
Jaguar I-PACE	`00:1a:37:70:●●:●●`

We were able to obtain the identifiers in 41 cases (76%)[8] from a variety of locations including the two-car arrangement shown in Figure 8. Here the identifiers for both vehicles were acquired from the same antenna position, suggesting that an attacker could simply park next to a charging station and collect identifiers as other users arrive subsequently providing them[9] in order to obtain free charging on another user's account. As the charging spots are operated by a single provider, the attacker can be confident of targeting valid customers.

User Tracking In the simplest attack, charging sessions are linked by monitoring a number of busy public chargers for the appearance of vehicle identifiers. From time-of-day, charge duration and location information, behavioural profiles can be inferred. The invasiveness of the attack increases where the attacker is able to match a vehicle identity to other data. Popular charger-sharing schemes [60] allow anyone to register their home or business charger as a public site; any user booking to charge can then be associated with their vehicle identifier and tracked at any monitored station. Monitoring a charger near a sensitive event such as a union meeting, protest gathering or compromising night-spot would reveal more personal information about an individual's habits.

With a wireless attack, a wardriving approach also allows an attacker to associate a vehicle with a street address. This could easily be conducted by a delivery driver or postal worker as they visit properties regularly. Known MAC allocations to manufacturers provide a coarse-grained indication of the vehicle as well, such as identifying expensive vehicles and then determining when they have been left in a public car park, or indeed when their owner is out of the house.

10 Lessons Learnt

The refinement of EV charging systems is still ongoing. In light of our observations, we have distilled a set of security lessons that can improve existing and future designs.

10.1 Wireless Threats

The most notable finding here is that the design of CCS communication allows a wireless attacker to observe it at a distance without prior interaction or tampering. In this case the attack was entirely passive, but has similar implications for the potential of active attacks that would currently be far more invasive. As in-vehicle wireless systems have been plagued by attacks in recent years, our results indicate that a testing model which considers emissions security as well as unwanted interference is crucial in future development.

10.2 Reliance on a Non-Existent PKI

The ISO 15118 security model, and thus that of CCS, relies on the existence of a complex PKI, to underpin TLS at the Transport Layer and XML Security for external message values at the Application Layer. The merits of that infrastructure are an ongoing topic of academic study [8, 72, 52], but its complexity also presents a more practical problem. At the time of writing, no widespread ISO 15118 PKI is deployed. While small-scale pilots have been attempted, there is still open debate about provision of the infrastructure and the authors are aware of public proposals from three different commercial entities to provide transaction brokerage and act as the Root Certification Authority [27]. There is even disagreement about the model the PKI will take; whether it will derive from a single root of trust, a consortium of trusted entities or some more open model [50]. Meanwhile the competing pressures to provide new functionality remain, spurring alternative solutions such as AutoCharge and encouraging service development without underlying security provision.

Even once a PKI is operating for public chargers in large charging networks, it remains unclear to what extent private units in individual homes or offices will benefit. A capacity for self-signed contract certificates to be manually installed into vehicles by users does exist, but unless contract-based billing is used ISO 15118 exempts charging installations from any security requirements; instead relying on the physical security of the location and cabling — which we have demonstrated to be insufficient. Manufacturer choices (and indeed user willingness) will determine whether private chargers can enjoy these security benefits.

It is important therefore to provide at least some security implementation that is decoupled from the need for access to a PKI. We discuss such an approach in Section 11.

10.3 Available PHY Security Disabled

The HomePlug GreenPHY (HPGP) PLC technology supports a *Secure SLAC* mode that protects the pairing and NMK distribution process, but this is disabled by specification in the ISO 15118 standard, relying instead on TLS for all security properties. While this can meet the charging use cases outlined in that standard, it leaves an opportunity for a pervasive security baseline completely ignored, despite proposing the communication channel for general use. All too of-

[8] 31 cases from SLAC initialisation messages and 10 more from network management messages

[9] Typically updating the MAC setting using `open-plc-utils` [45] and a serial debug port over UART or SPI [21]

ten history has shown that leaving security to individual developers atop insecure platforms produces widespread security problems, even more so when the channel is considered physically private.

11 Countermeasures

To mitigate the unintended wireless channel, familiar emissions security mechanisms such as chokes or shielding can be applied to reduce leakage [7], although hardware modifications for existing systems are costly and time-consuming. Some proposals for future, high-power chargers include liquid-cooled charging cables and we would expect this to attenuate the signals if the cooling jacket wraps the communication lines as well as the power-delivery ones. This would not eliminate emissions from the vehicle or charger circuitry however, nor is it likely to exist in smaller, private chargers.

At a network level, we have argued for the use of the available HPGP security mechanisms above, but note that in their present form they are still reliant on a PKI to function. In addition the HPGP key distribution behaviour itself introduces an unnecessary risk of interception. Whether the SLAC protocol operates in its secure mode or not, it is still unilateral: the charger generates a network key and then provides it to the vehicle. However, the SLAC process is typically implemented in software by the same devices that undertake the higher-level ISO 15118 communication, including possible TLS sessions, and as such require the capabilities for an Elliptic Curve Diffie-Hellman key derivation for AES128 [48].

We propose additional steps in the SLAC initialisation, as a fallback to provide confidentiality from the MAC-layer upwards in the event that PKI access is unavailable. Figure 11 shows the modified protocol. Upon receiving a network match request, the charger generates an Elliptic-Curve keypair (d_C, Q_C) and instructs the vehicle to commence a key exchange, along with Q_C. If the vehicle also supports the protocol then it generates (d_V, Q_V) and responds with Q_V. The derived key becomes the new NMK and the charger blanks the NMK field in the subsequent `CM_SLAC_MATCH.CNF` message. If the vehicle does not support the protocol then the unrecognised message will be dropped. The charger maintains a timeout counter after step 6.1 and, upon expiry, falls back to the existing protocol's step 7.

While it cannot provide authentication and therefore cannot mitigate man-in-the-middle attacks, the threat of passive eavesdropping is eliminated using this approach. By building only on existing functionality, the protocol is deployable in existing vehicles as well as new ones.

12 Conclusion

We have demonstrated that use of PLC in EV charging and the design of the CCS standard lead to a uniquely high-quality, unintentional wireless channel. We have evaluated the susceptibility of real-world chargers and found a reliable channel in every case. Although conditions vary substantially between sites, for eavesdropping we achieved a peak successful recovery rate of 100% in one case and could intercept traffic several metres from the target, in a different parking bay, with a rate of 91.8%. We showed how a series of further design choices allow recovery of network keys and passive monitoring of all traffic in plaintext. We presented lessons learnt and potential improvements to mitigate the problems so that they do not hinder the secure adoption of global EV charging infrastructure by the growing number of EV owners worldwide.

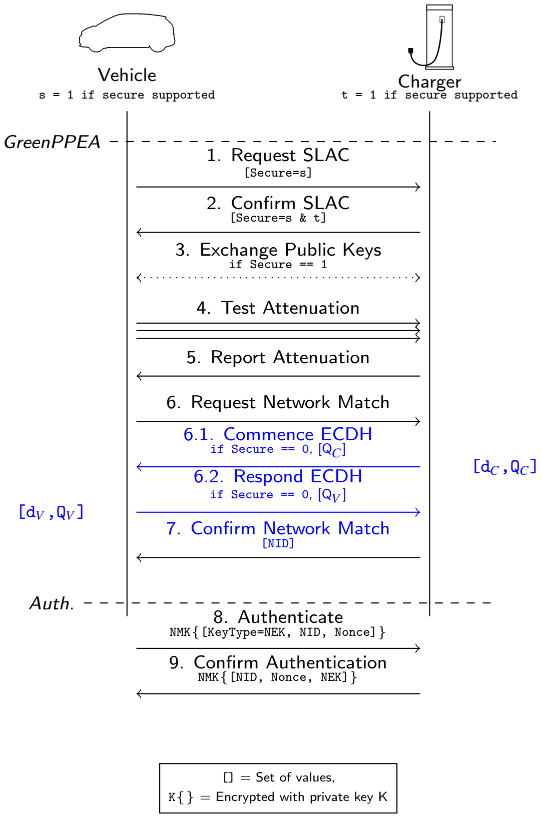


Figure 11: The modified SLAC network establishment. Steps 6.1 and 6.2 are new, while step 7 has been modified.

Acknowledgements

Richard Baker was supported by the EPSRC.

Disclosure Statement

We disclosed our findings to the tested vehicle and charger manufacturers, along with AutoCharge operators.

References

[1] ABB. Terra 53 Product Leaflet, 2017.

[2] International Energy Agency. Global EV Outlook 2018, 2018.

[3] Monjur Alam, Haider Adnan Khan, Moumita Dey, Nishith Sinha, Robert Callan, Alenka Zajic, and Milos Prvulovic. One&done: A single-decryption em-based attack on openssls constant-time blinded RSA. In *27th USENIX Security Symposium*, pages 585–602, 2018.

[4] Cristina Alcaraz, Javier Lopez, and Stephen Wolthusen. Ocpp protocol: Security threats and challenges. *IEEE Transactions on Smart Grid*, 8(5):2452–2459, 2017.

[5] HomePlug Powerline Alliance. HomePlug Green PHY Specification. *HomePlug, June*, 2010.

[6] AMO Labs. Amo labs preparing to enter the european market with gridwiz!, 2018.

[7] Ross Anderson. *Security engineering*. John Wiley & Sons, 2008.

[8] Kaibin Bao, Hristo Valev, Manuela Wagner, and Hartmut Schmeck. A threat analysis of the vehicle-to-grid charging protocol iso 15118. *Computer Science-Research and Development*, 33(1-2):3–12, 2018.

[9] BBC. Petrol and diesel ban: How will it work?, 2017. https://www.bbc.co.uk/news/uk-40726868.

[10] Cesar Bernardini, Muhammad Rizwan Asghar, and Bruno Crispo. Security and privacy in vehicular communications: Challenges and opportunities. *Vehicular Communications*, 2017.

[11] Bastian Bloessl, Michele Segata, Christoph Sommer, and Falko Dressler. An ieee 802.11 a/g/p ofdm receiver for gnu radio. In *Proceedings of the second workshop on Software radio implementation forum*, pages 9–16. ACM, 2013.

[12] BP Chargemaster. Chargemaster Ultracharge 500S Datasheet, 2019.

[13] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 163–177. ACM, 2018.

[14] Chargemaster Ltd. Polar network, 2018. https://chargemasterplc.com/polar/.

[15] Chargepoint Services. Geniepoint, 2019. https://www.chargepointservices.co.uk.

[16] CharIn. Target grid integration levels, 2019. https://insideevs.com/ccs-combo-standard-v2g-2025/.

[17] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, volume 4, pages 447–462. San Francisco, 2011.

[18] Mark Chediak. Electrify america plans $200 million for california clean cars, 2019. https://www.bloomberg.com/news/articles/2018-10-03/electrify-america-plans-200-million-for-california-clean-cars.

[19] Matthias Dalheimer. Ladeinfrastruktur fr elektroautos: Ausbau statt sicherheit, 2017. https://media.ccc.de/v/34c3-9092-ladeinfrastruktur_fur_elektroautos_ausbau_statt_sicherheit.

[20] DBT. Quick Charger Dual DC Product Datasheet, 2014.

[21] devolo AG. dLAN Embedded PLC Module Datasheet, 2012. https://www.codico.com/shop/media/datasheets/Devolo_dLAN_Green_PHY_Module_20130713_en_data_sheet_019.pdf.

[22] EcoG. Providing a customized electric vehicle (ev) fast charging experience through a paas for value added services & shared revenue streams, 2019.

[23] Ecotricity. Electric highway, 2018. https://www.ecotricity.co.uk/for-the-road.

[24] Efacec. Efacec QC45 Datasheet, 2016.

[25] Efacec. QC45S Product Page, 2019. https://electricmobility.efacec.com/ev-qc24s-quick-charger/.

[26] ElaadNL. Iota charging station, 2018.

[27] ElaadNL. Update Global EV Charging Test: PKI Workshop, 2018.

[28] Engadget. California bill would ban new fossil fuel vehicles from 2040, 2018. https://www.engadget.com/2018/01/04/california-bill-would-ban-new-fossil-fuel-vehicles-from-2040/.

[29] European Alternative Fuels Observatory. Electric vehicle charging infrastructure, 2018.

[30] CharIN e.V. What is the combined charging system?, 2018. https://www.charinev.org/ccs-at-a-glance/what-is-the-ccs/.

[31] EVTRONIC. Quickcharger product datasheet, 2016.

[32] Rainer Falk and Steffen Fries. Electric vehicle charging infrastructure security considerations and approaches. *Proc. of INTERNET*, pages 58–64, 2012.

[33] Fastned. Autocharge, 2019. https://support.fastned.nl/hc/en-gb/articles/115012747127-Autocharge-.

[34] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2011.

[35] Achim Friedland. Security and privacy in the current e-mobility charging infrastructure, 2016. https://blog.deepsec.net/deepsec2016-talk-security-privacy-current-e-mobility-charging-infrastructure-achim-friedland/.

[36] Harald T Friis. A note on a simple transmission formula. *proc. IRE*, 34(5):254–256, 1946.

[37] Flavio D Garcia, David Oswald, Timo Kasper, and Pierre Pavlidès. Lock it and still lose iton the (in) security of automotive remote keyless entry systems. In *25th USENIX Security Symposium*, 2016.

[38] Jonathan M. Gitlin. Electrify america will deploy 2,000 350kw fast chargers by the end of 2019, 2018. https://arstechnica.com/cars/2018/04/electrify-america-will-deploy-2000-350kw-fast-chargers-by-the-end-of-2019/.

[39] Mordechai Guri, Matan Monitz, and Yuval Elovici. Usbee: Air-gap covert-channel via electromagnetic emission from usb. In *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*, pages 264–268. IEEE, 2016.

[40] Christina Höfer, Jonathan Petit, Robert Schmidt, and Frank Kargl. Popcorn: Privacy-preserving charging for emobility. In *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*, pages 37–48. ACM, 2013.

[41] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *IEEE Security & Privacy*, (3):49–55, 2004.

[42] InsideEVs. Tesla model 3 with ccs combo inlet, s & x with ccs adaptor in europe, 2019. https://insideevs.com/tesla-model-3-ccs-combo-s-x-adaptor/.

[43] InstaVolt. Our technology, 2018. https://instavolt.co.uk/about-us/our-technology/.

[44] InstaVolt Ltd. About InstaVolt, 2018. https://instavolt.co.uk/.

[45] INSYS MICROELECTRONICS GmbH. INSYS Powerline GP Manual, 2017. https://256.insys-icom.com/bausteine.net/f/10637/HB_en_INSYS_Powerline_GP_1711.pdf?fd=0.

[46] Rob Millerb Ishtiaq Roufa, Hossen Mustafaa, Sangho Ohb Travis Taylora, Wenyuan Xua, Marco Gruteserb, Wade Trappeb, and Ivan Seskarb. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *19th USENIX Security Symposium, Washington DC*, pages 11–13, 2010.

[47] Road vehicles Vehicle to grid communication interface Part 1: General information and use-case definition. Standard, International Organization for Standardization, Geneva, CH, 2013.

[48] Road vehicles Vehicle to grid communication interface Part 2: Network and application protocol requirements. Standard, International Organization for Standardization, Geneva, CH, 2014.

[49] Mohammad Khodaei, Hongyu Jin, and Panagiotis Papadimitratos. Secmace: Scalable and robust identity and credential management infrastructure in vehicular communication systems. *IEEE Transactions on Intelligent Transportation Systems*, 19(5):1430–1444, 2018.

[50] Paul Klapwijk and Lonneke Driessen-Mutters. Exploring the public key infrastructure for iso 15118 in the ev charging ecosystem, 2018.

[51] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost talk: Mitigating emi signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159. IEEE, 2013.

[52] Seokcheol Lee, Yongmin Park, Hyunwoo Lim, and Taeshik Shon. Study on analysis of security vulnerabilities and countermeasures in iso/iec 15118 based electric vehicle charging technology. In *IT Convergence and Security (ICITCS), 2014 International Conference on*, pages 1–4. IEEE, 2014.

[53] Michael Himmels. Devolo real world field tests, 2011. http://www.homeplug.org/media/filer_public/25/4f/254f6adb-096a-4913-842b-91e3775da045/devolo_presentation.pdf.

[54] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. Private memoirs of a smart meter. In *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, pages 61–66. ACM, 2010.

[55] Marc Mültin. *Das Elektrofahrzeug als flexibler Verbraucher und Energiespeicher im Smart Home*. PhD thesis, KIT-Bibliothek, 2014.

[56] Open Fast Charging Alliance. Automatic charging start and authorization of electric vehicles, 2017.

[57] Organisation Internationale des Constructeurs d'Automobiles. World Motor Vehicle Production: World Ranking of Manufacturers, 2016.

[58] Johan Peeters. Fast charging just got faster. Presentation at eMove360 Conference 2017.

[59] POD Point. Open charge electric car charging stations, 2018. https://pod-point.com/open-charge.

[60] Recargo Inc. PlugShare, 2018. https://www.plugshare.com/.

[61] Reuters. Paris plans to banish all but electric cars by 2030, 2017. https://www.reuters.com/article/us-france-paris-autos/paris-plans-to-banish-all-but-electric-cars-by-2030-idUSKBN1CH0SI.

[62] Zeinab Rezvani, Johan Jansson, and Jan Bodin. Advances in consumer electric vehicle adoption research: A review and research agenda. *Transportation research part D: transport and environment*, 34:122–136, 2015.

[63] Matthias Schulz, Patrick Klapper, Matthias Hollick, Erik Tews, and Stefan Katzenbeisser. Trust the wire, they always told me!: On practical non-destructive wire-tap attacks against ethernet. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 43–48. ACM, 2016.

[64] Share&Charge. Share&charge, 2019. https://shareandcharge.com/.

[65] Shell Plc. Welcome to shell recharge, 2019. https://www.shell.co.uk/motorist/welcome-to-shell-recharge.html.

[66] Peter Smulders. The threat of information theft by reception of electromagnetic radiation from rs-232 cables. *Computers & Security*, 9(1):53–58, 1990.

[67] U.S. Department of Energy Alternative Fuels Data Centre. Alternative fueling stations, 2018. https://www.afdc.energy.gov/stations/.

[68] Wim Van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985.

[69] David Varodayan and Ashish Khisti. Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage. In *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, pages 1932–1935. IEEE, 2011.

[70] Roel Verdult, Flavio D Garcia, and Josep Balasch. Gone in 360 seconds: Hijacking with hitag2. In *21st USENIX Security Symposium*, pages 237–252, 2012.

[71] Brad Zarikoff and David Malone. Experiments with radiated interference from in-home power line communication networks. In *Communications (ICC), 2012 IEEE International Conference on*, pages 3414–3418. IEEE, 2012.

[72] Daniel Zelle, Markus Springer, Maria Zhdanova, and Christoph Krauß. Anonymous charging and billing of electric vehicles. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, page 22. ACM, 2018.

[73] Kexiong (Curtis) Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, and Yaling Yang. All your GPS are belong to us: Towards stealthy manipulation of road navigation systems. In *27th USENIX Security Symposium*, pages 1527–1544, Baltimore, MD, 2018. USENIX Association.

[74] ZF Car eWallet GmbH. Car ewallet, 2019. https://car-ewallet.de/index.php/what-we-do/.

Appendices

A CCS Circuit Design

Figure 12 shows the communication circuit for PLC in CCS charging systems, including the connection of the circuit to the Control Pilot and Protective Earth lines, along with the additional components affecting the Control Pilot line due to the need for backwards-compatibility with the IEC 61851 communication that shares the lines.

B HomePlug GreenPHY Receiver

In this section we describe our eavesdropping tool in detail. As noted in Section 6, the tool is effectively a modified receiver design, although newly-implemented entirely in software. Since HomePlug GreenPHY (HPGP) [5] is an orthogonal frequency-division multiplexing (OFDM) technology, many elements of the tool structure are similar to a Wi-Fi receiver.

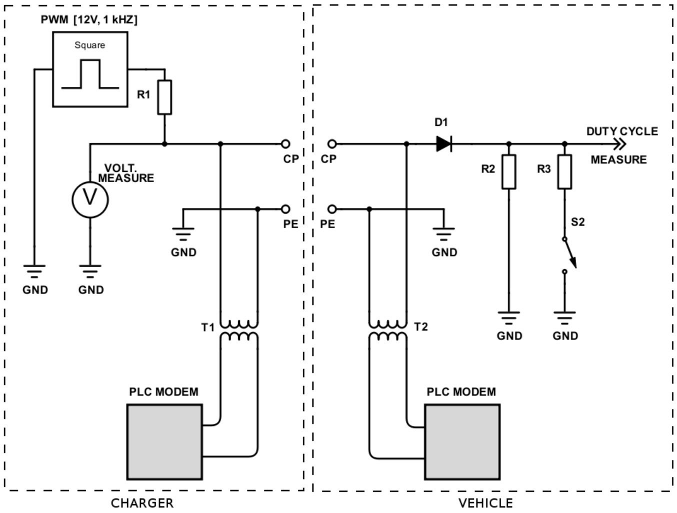


Figure 12: A diagram of the CCS communication circuit. The loads on each line connected to the PLC modem are not balanced. Resistors R2 & R3 alter the voltage in the low-level communication, but also vary the imbalance further.

Raw signals are first collected using a suitable capture device. A Rigol DSA-2302A oscilloscope was used in our testbed arrangement, as can be seen in Figure 13. Even here the radiated emissions were easily observed; the yellow line in the figure represents the conducted signal, while the blue line is the radiated signal received by a short random-wire antenna. Although the distance shown here is very short, we were still able to observe the signal from the other side of the lab, several metres away. We later employed software-defined radios for signal capture, for their ability to receive and stream a captured signal in real time.

The captured signal is filtered in the frequency domain, benefiting from knowledge of the active regions of the HPGP band and the ability to survey initially an individual site's leakage before eavesdropping in earnest. A sharp-edged digital filter is used to remove regions with notable interference ingress or where channel gain is so low as to provide no useful information. The signal is then resampled into the HPGP native timebase of 75MHz.

Frame Detection and Time Alignment With the signal suitably pre-filtered and digitised, the PPDUs are detected using a *Double Sliding-Window* power detector; a design that accurately identifies the rise in power that accompanies the start of a packet. The detector calculates the power of the incoming signal and maintains two windows A and B of equal length L that are arranged with a time lag such that calculated power levels are included in window A at time t, subsequently passing out of window A and into window B at time $t+L$ and out of the detector entirely at time $t+2L$. At each sample, the power in each window is updated and the total power in A is divided by that in B. This configuration causes the output signal to spike quickly on increases in power levels, while remaining stable at equal power levels (i.e., prior to or during a frame). By selecting an appropriate value of L (based on the frame's structure), transient noise can be prevented from triggering a frame.

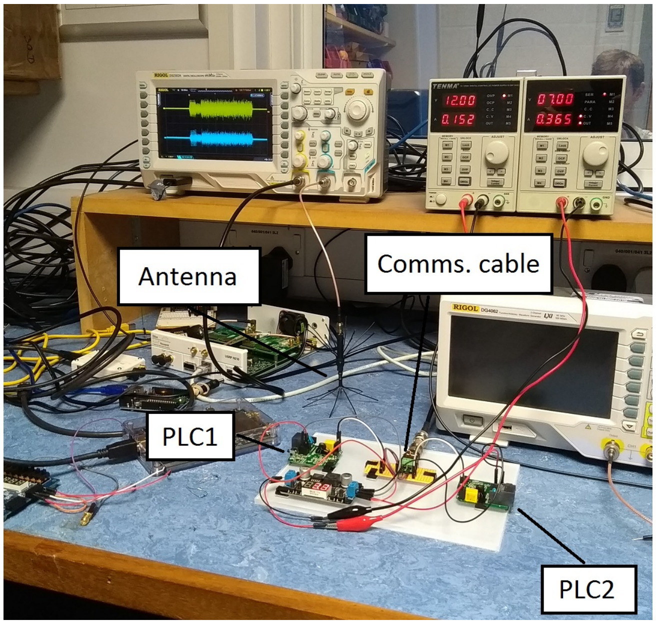


Figure 13: HomePlug AV adaptors communicating across a short wire. Conducted signals and radiated emissions can be seen on the oscilloscope (top in yellow and bottom in blue, respectively).

OFDM requires precise time synchronisation in order to demodulate correctly. We performed this by correlating the entire preamble against a template, which provided sample-accurate alignment.

CPO, SCO & Channel Estimation In practice, a transmitter and receiver in an OFDM system will have neither precisely-aligned oscillators nor synchronised sample clocks, leading to Carrier Phase Offset (CPO) and Sampling Clock Offset (SCO). CPO causes an apparent frequency offset for the entire received signal, meaning that the frequency-domain representation exhibits a phase rotation. Meanwhile, SCO leads to an apparent phase drift across subcarriers in the frequency domain. Both phenomena hamper demodulation and must be corrected beforehand. Channel estimation is also crucial to successful reception; assessing the gain and phase alterations that have been experienced by the signal due to the propagation environment.

Our receiver estimates the CPO using a method derived from Bloessel et. al.'s work; estimating the CPO using the seven full-amplitude SYNCP preamble symbols in place of the Wi-Fi short-training sequence [11] (omitting the initial

192 as they have been windowed in symbol shaping):

$$cpo_{est} = \frac{1}{384} Arg \left(\sum_{i=0}^{7 \cdot 384} x[i] \bar{x}[i+384] \right)$$

where x is the received signal samples.

From the extracted section of the preamble, complex samples are multiplied with the conjugate of the same sample in the next SYNCP block. This produces an estimate of the phase progression introduced between those SYNCP blocks by the mismatch between transmitter and receiver (plus noise). Dividing through by the length of the SYNCP block gives an estimate of the phase offset per sample. The length of the sequence (2688) and the number of repetitions (7) permit an accurate CPO estimate. The per-sample CPO estimate can then be used to correct the remainder of the captured signal.

$$x[i] \leftarrow x[i] \cdot e^{-jcpo_{est} i}$$

As the estimated CPO will not precisely match the actual CPO, ongoing correction is applied to each received symbol by estimating the CPO between the cyclic prefix and the symbol tail, with a suitable correction being applied over that symbol.

$$cpo_{estcp} = \frac{1}{3072} Arg \left(\sum_{i=0}^{GI} x[i] \bar{x}[i+3072] \right)$$

where GI is the guard interval (with four values depending on the symbol and system settings).

The channel estimation is performed in the frequency domain, by comparing the received preamble symbols to a locally-computed template. HPGP provides no pilot symbols so all estimation must be performed from the preamble and maintained across the PPDU. The results for each preamble symbol are averaged and a channel estimate from the active preamble subcarriers computed. From this a channel estimate for the full channel is derived by interpolation, while the SCO is estimated from the slope of the phase differences in the channel estimate. As the CPO and SCO are due to hardware imperfections in the transmitter and receiver, rather than channel properties, estimates are maintained between received PPDUs by way of a moving average. The channel estimate, by contrast, is discarded after a PPDU has been received.

Demodulation Demodulation takes place in the frequency domain (via a 3072-point DFT), after the removal of the cyclic prefix for the symbol and correction for the channel effects at each subcarrier. As HPGP uses QPSK modulation, the receiver compares the measured value for the subcarrier in the in-phase and quadrature channels to the nominal values and estimates, under an additive white Gaussian noise assumption, the likelihood of the transmitted value having been a 0 or 1 bit. These probabilities are expressed as a ratio, the Log Likelihood Ratio (LLR) and then scaled according to the gain for the subcarrier in the channel estimate, such that the uncertainty inherent in weakly-received subcarriers is represented.

Post Processing Demodulated soft bits are combined by averaging to benefit from HPGP's redundancy schemes. They are then rearranged in read-by-row-write-by-column fashion to undo the channel interleaving process.

The FEC decoding is applied to produce hard decisions about the bit values. HPGP uses an unpunctured Turbo code with two systematic, rate $\frac{2}{3}$ constituent codes. Each pair of input bits (i, j) produces a codeword (i, j, p, q), where p and q are parity bits, p from the in-order input and q from an interleaved input.

Finally, the bits are unscrambled by XORing with the same generator polynomial used in the transmitter to recover the original sequence.

The CRC checks are computed over the received bits to determine if the contents have been received successfully, however the PHY-layer bits are delivered to the higher layers irrespective as even messages containing errors may provide useful information.

Each stage of the receiver is configurable with a wide range of parameters. In particular, the power threshold to trigger PPDU capture, the frequency-domain filtering, the initial CPO estimate and the estimated noise variance for demodulation all permit tailoring the receiver to a given scenario.

Considering the emissions as a wireless channel, the simple modulation and redundancy in HomePlug GreenPHY's robust ("ROBO") transmission modes mean the attacker need not match the channel characteristics of any particular receiver; they need only to receive the transmissions with enough of the signal intact. Specifically, the attacker requires a positive signal-to-noise ratio (SNR) over some fraction B of the transmitted bandwidth. The selection of B depends upon the transmissions mode in use and the effectiveness of any error-correction mechanisms, however for a rough estimate the level of redundancy can be used. Thus for `MINI_ROBO`, `STD_ROBO`, `HS_ROBO` B can be taken as 5.2MHz, 6.5MHz, 13MHz ($\frac{1}{5}$, $\frac{1}{4}$ and $\frac{1}{2}$ of the 26 MHz HPGP bandwidth) respectively.