PLC COMMUNICATION FOR EMOBILITY

Qualcomm PLC Sniffer

RAKwireless LX200V50 EVB · Qualcomm QCA7550 · Firmware v5.1.0 · HomePlug Green PHY · ISO 15118

CONTENTS

01 Direct connection for traffic capture 2

02 Inductive connection 4

03 Measurement procedure 5

04 Capture analysis 6

INTRODUCTION

The Qualcomm PLC Sniffer captures HomePlug Green PHY communication between a plug-in electric vehicle (PEV) and a charging station (EVSE). It supports R&D debugging, development and diagnostic field testing of charging sessions.

The RAKwireless LX200V50 EVB runs Qualcomm PLC Sniffer firmware v5.1.0 on the QCA7550 modem. Received traffic is delivered to a computer through the RJ45 Ethernet port for recording and analysis.

The sniffer must be operating before SLAC starts. During SLAC (ISO 15118-3), the EVSE sends the network membership key (NMK) to the PEV in `CM_SLAC_MATCH.CNF`. The sniffer listens for this message and uses the NMK to join the AVLN (HomePlug AV logical network) and decrypt the PLC traffic. The decrypted traffic is forwarded as Ethernet frames to the PC, which captures it with the network interface in promiscuous mode.

Traffic of interest: SLAC management frames, IPv6/ICMPv6, SECC Discovery Protocol (SDP), TCP/TLS and Ethernet payloads carrying ISO 15118-2, ISO 15118-20 or DIN 70121.

This document describes the direct connection of the sniffer for traffic capture (section 01), the inductive connection (section 02), the measurement procedure (section 03) and the analysis of the capture (section 04).

01

Direct connection for traffic capture

BOARD ORIENTATION AND PLC INPUT

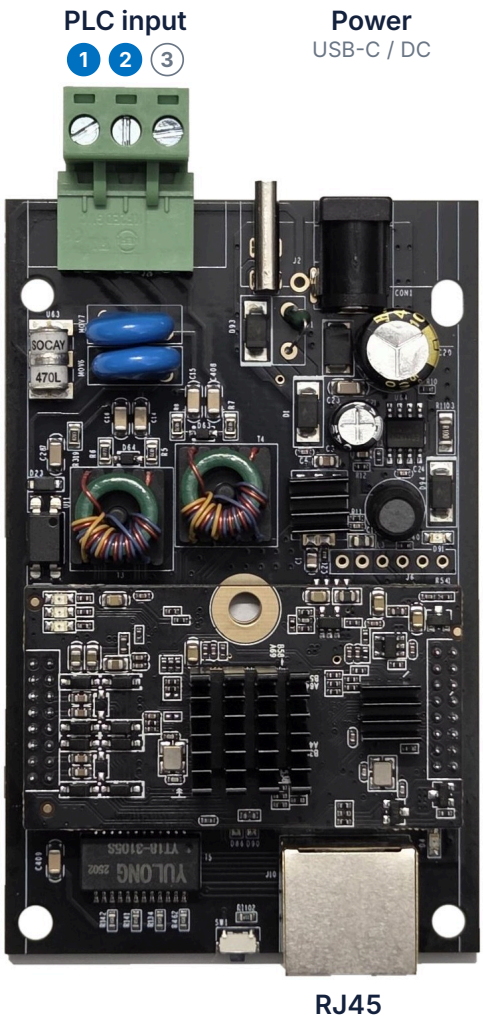


Figure 1 · LX200V50 EVB, component side: PLC input positions 1–3, power and RJ45

Figure 1 shows the board from the component side, with the green terminal at the top and the RJ45 connector at the bottom.

The Qualcomm PLC Sniffer firmware uses channel 1 of the QCA7550 for sniffing. Therefore, connect CP and PE to **positions 1 and 2** (left and centre contacts):

POSITION	SIGNAL
1	**CP** (Control Pilot)
2	**PE** (Protective Earth)
3	Unused

POWER AND ETHERNET

Power	Use an isolated, regulated 5V USB-C supply or the matching DC adapter for the supplied board revision. Use only one power input at a time. Keep the heat sink clear.
Ethernet	Connect the RJ45 port directly to the PC or to its USB Ethernet adapter. Capture on that interface in promiscuous mode; an IP address is not required for raw Ethernet capture.

DIRECT CONNECTION TO CP/PE WIRES

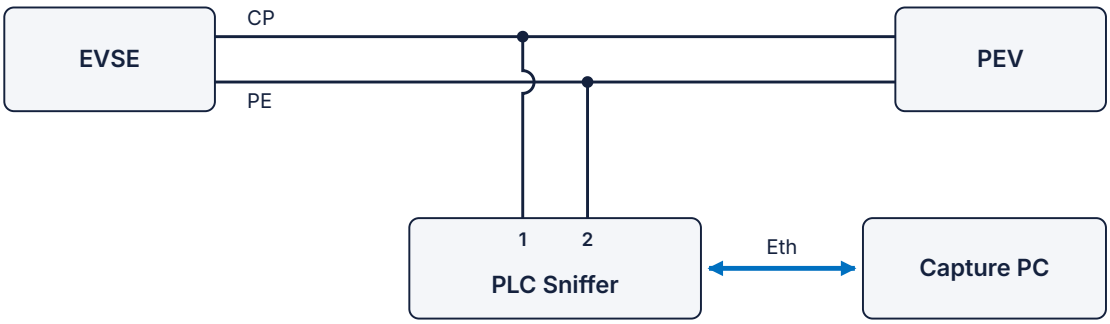


Figure 2 · Direct connection: sniffer connected in parallel to CP and PE

IMPORTANT

Connect only to CP and PE. Preserve the charging connection and PE continuity.
Make or change the direct wiring with the charger de-energized.

COAXIAL CONNECTION

The BNC-to-screw-terminal adapters shown in Figure 3 are included in the box. With a short 50 Ω coaxial cable, they can be used both for the direct connection to CP and PE and for the inductive signal pickup (section 02).

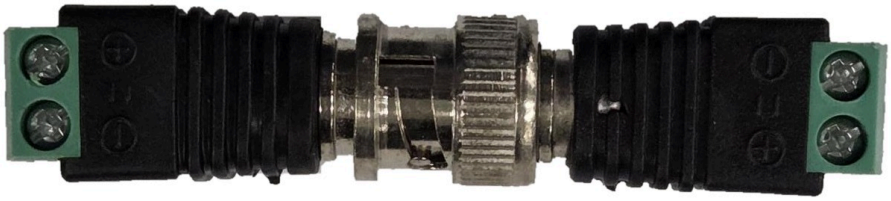


Figure 3 · BNC-to-screw-terminal adapters included in the box

Wire the adapter to the sniffer terminal as follows:

Pos. 1	Connect the BNC centre conductor / “+” to position **1** (CP).
Pos. 2	Connect the BNC shell and shield / “−” to position **2** (PE).

For the direct connection, connect the centre conductor to CP and the shield to PE at the other end of the coax.

NOTE

Verify the continuity of the adapter. The adapter provides a connection only; it does not provide isolation.

02

Inductive connection

INDUCTIVE PICKUP – ACCESS TO THE CABLE EXTERIOR

If the exterior of the charging cable is accessible, the PLC signal is picked up by a coupler around the cable. The coupler is connected to input positions 1 and 2 of the sniffer, directly or with a 50 Ω coaxial cable (see section 01). The sniffer is powered separately.

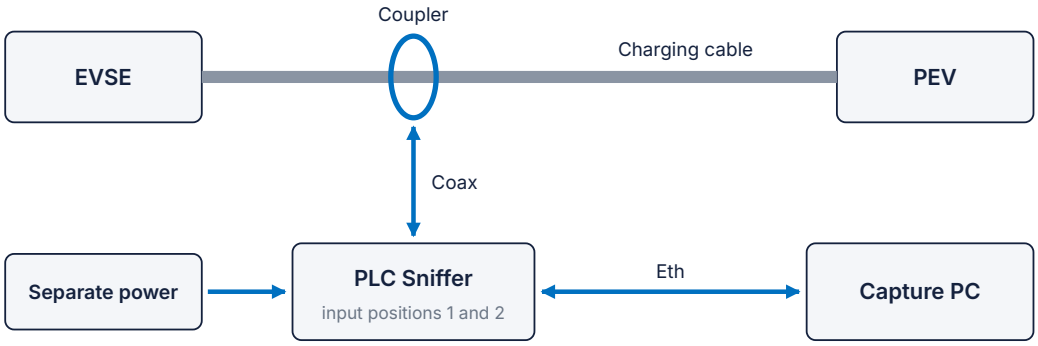
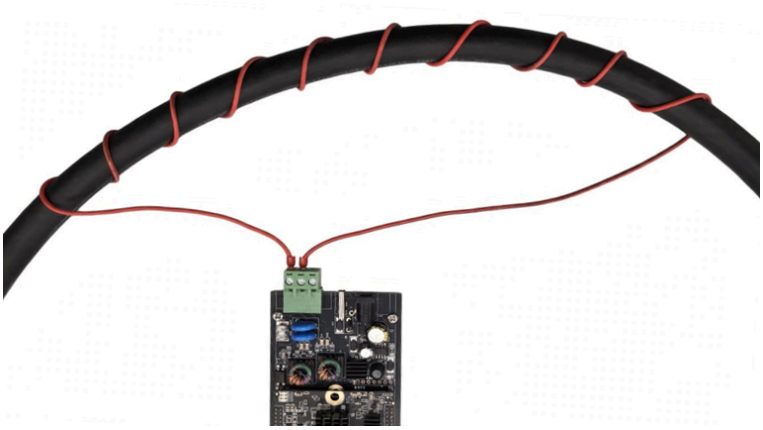


Figure 4 · Test setup with inductive pickup

PICKUP OPTIONS



Wire pickup

Wind about 10 turns of insulated wire over a length of about 50 cm around the intact cable jacket. Connect the two winding ends to positions 1 and 2 of the sniffer, directly or via the coax and the BNC adapter. Keep the two leads apart; do not twist them.



Gossen AC clamp



PREMO MICU 300A

Figure 5 · Pickup options: wire pickup, Gossen AC clamp and PREMO MICU 300A

03
Measurement procedure

EQUIPMENT

Sniffer	Qualcomm PLC Sniffer: RAKwireless LX200V50 EVB with Qualcomm PLC Sniffer firmware v5.1.0.
Power	Isolated, regulated 5V USB-C supply or the matching DC adapter.
PC	Computer with Wireshark, connected to the RJ45 port of the sniffer.
Connection	Direct (section 01) or inductive (section 02) connection to CP/PE.

MEASUREMENT STEPS

1. **Prepare the capture computer.** Install Wireshark and its capture driver. To decode charging messages, install a compatible ISO 15118 / DIN 70121 dissector such as dsV2Gshark.
2. **Connect before SLAC starts.** Attach the selected pickup, connect the Ethernet cable and power up the sniffer. Select the correct Ethernet interface, enable promiscuous mode and leave the capture filter empty.
3. **Start recording, then start charging.** The sniffer needs `CM_SLAC_MATCH.CNF` to join the AVLN and obtain the PLC encryption key. If the sniffer is connected after SLAC, restart the charging session.
4. **Check reception and save.** Look for SLAC, then IPv6/SDP and TCP traffic. Stop the capture after reproducing the issue and save it as `.pcapng`. Record the PEV, the EVSE, the pickup position, the firmware version and the time of the fault.

SNIFFER BEHAVIOUR

SLAC monitoring is passive. To read PLC-encrypted data, the sniffer joins the AVLN and sends the required management traffic. The firmware blocks Ethernet-to-PLC data injection.

ALTERNATIVE: TCPDUMP ON LINUX

On Linux, the capture can also be recorded with tcpdump:

```
sudo tcpdump -i eth0 -s 0 -U -w plc-session.pcap
```

Replace `eth0` with the name of the connected interface.

04
Capture analysis

Figure 6 shows a Wireshark example of ISO 15118-2 messages decoded with the dsV2Gshark dissector.

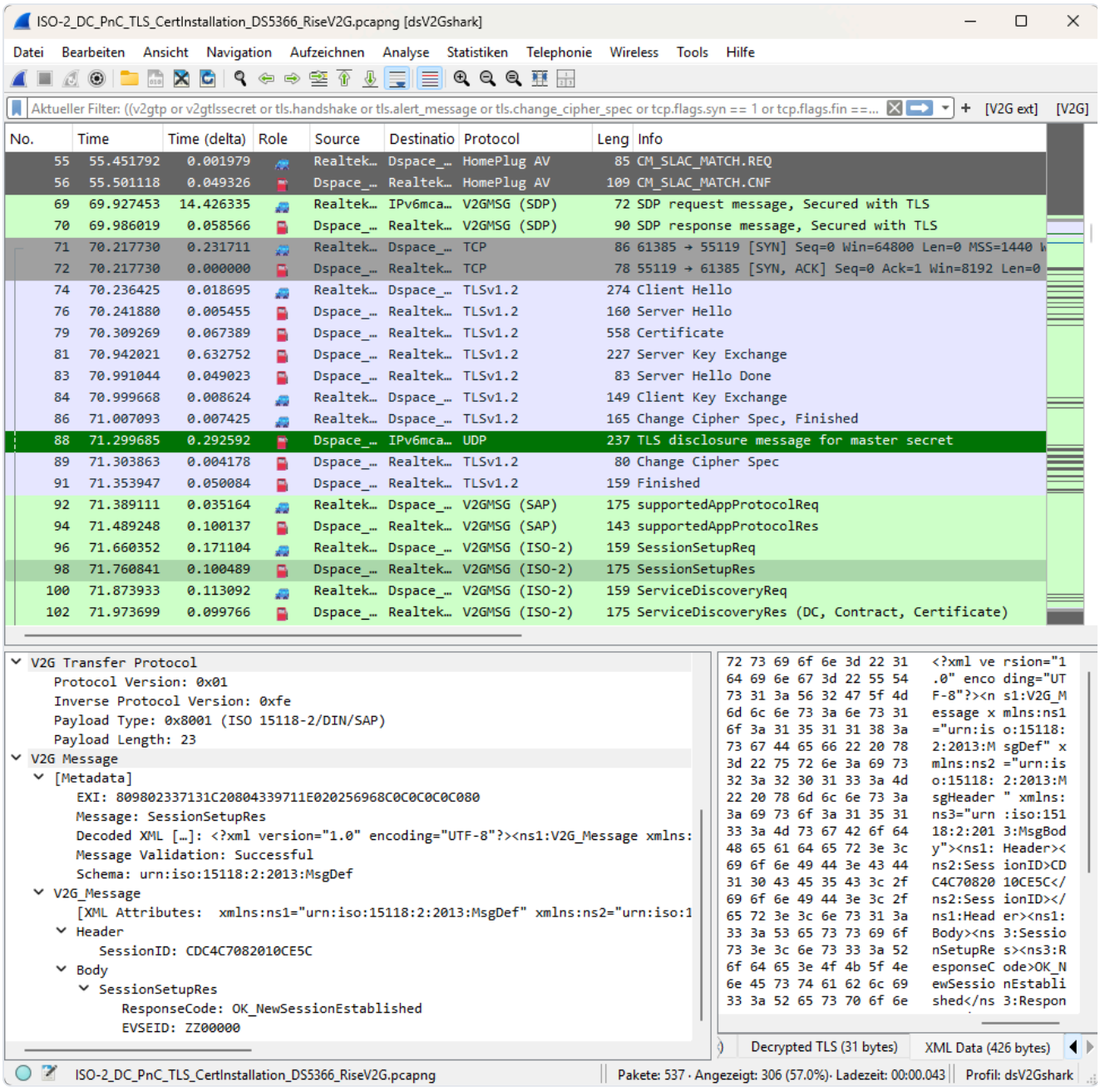


Figure 6 · Public dSPACE demonstration capture: SLAC, SDP, TLS and decoded ISO 15118-2 messages

The dsV2Gshark dissector is available at https://github.com/dspace-group/dsV2Gshark.