Smart grid (in)security

Sébastien Dudek

CiderSecurityCon, March 14th 2020

Who am I

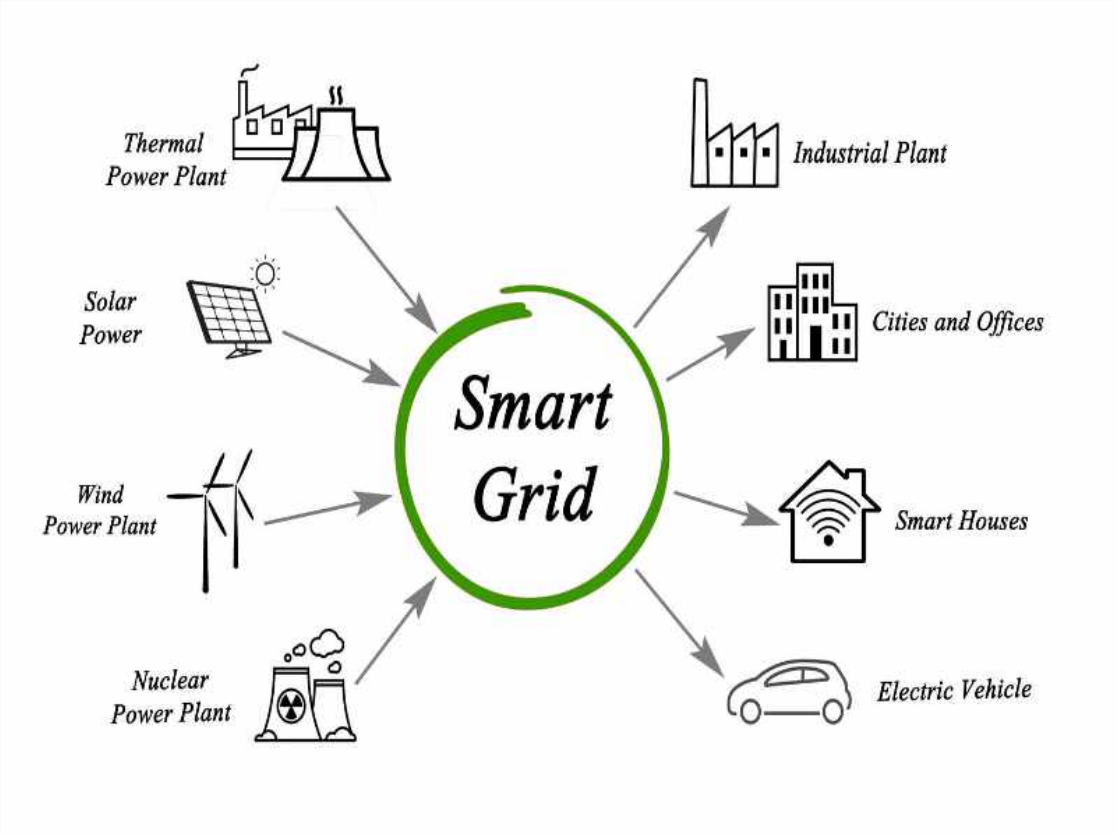
- Sébastien Dudek (@FlUxIuS)
- Founded PentHertz: RF and hardware security company
  - Pentests and Red Team tests
  - Researches
  - Trainings
  - HW & SW tools
- Interests: SDR, Hardware, RFID, Wi-Fi, 2G/3G/4G/5G, Bluetooth, LoRa, mobile networks, etc.

PentHertz

Smart Grids

Introduction

- Energy distribution which aims to be ”smart”
- Sensors and transmission + analysis devices → production + consumption
- Implemented Smart City compliant areas



Source: smart-energy.com

Why?

- Mainly to avoid issues in the past → power outage (e.g Northeast blackout of 2003[1])
- Many issues:
  - Cable expansion due to heat rise → sags between supporting structure → flashover
  - Flashover → triggers protection relays
  - If the other lines do not have enough spare capacity → cascading failure
- Need to use efficiently “smart” technologies for:
  - Wide variety of generation sources
  - Distribution assets coordination
  - Predict and control power consumption
  - Use energy storages for renewable energy production systems...

[1] https://www.scientificamerican.com/article/2003-blackout-five-years-later/

Smart grids

- Aims to manage small scale energy production nodes
- Manages the storage and distribution
- Use these nodes effectively
- Includes:
  - smart meters
  - smart appliances
  - renewable energy resources
  - and energy-efficient resources

Smart meters

Smart meters

- Official householders benefits:
  - estimated bills
  - better manage their energy purchases...
- The main purpose is to match consumption with generation
- Different prices according to time
- Data management: HomePlug (AV/GP)/IEEE 1901 and ITU-T G.hn

Source: https://en.wikipedia.org/wiki/Smart_meter

Smart meters (2)

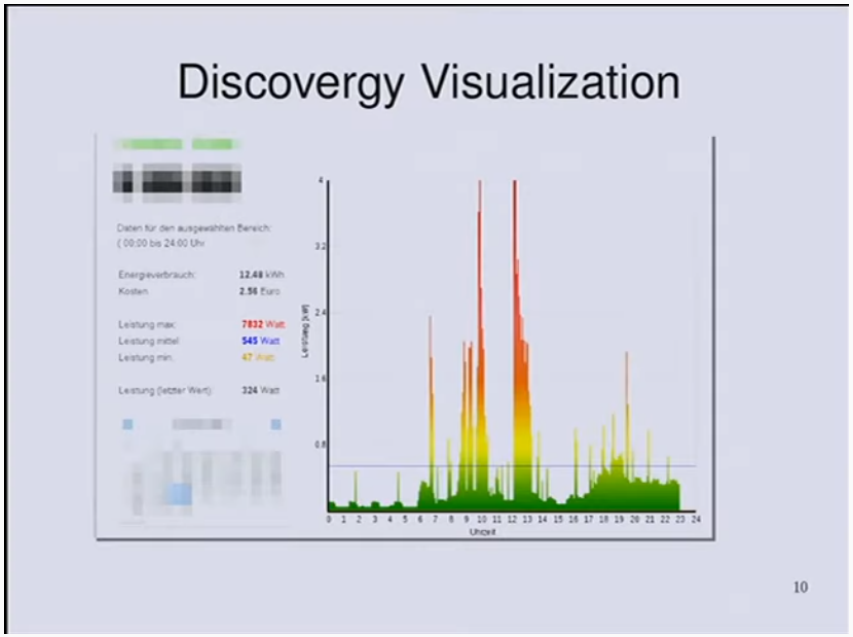
But there is also Wi-Fi, LoRa, ZigBee, GSM/GPRS, etc.

Source: Netanel Rubin at 33c3

And issues regarding ZigBee and GSM/GPRS connections

Smart meters: Discovergy case

Consumption plots exposed on Discovergy web interface:

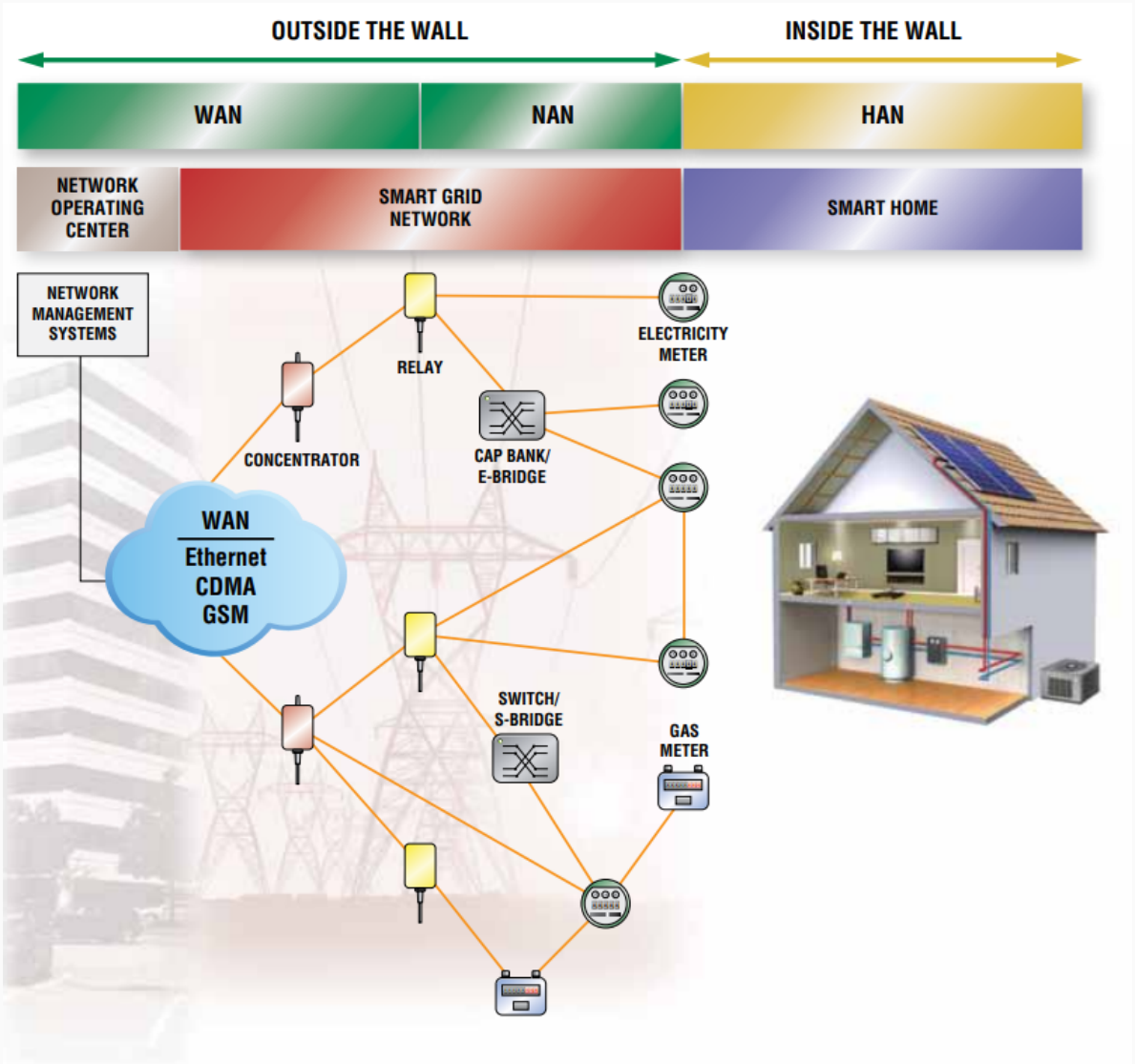


Source: Dario Carluccio and Stephan Brinkhaus at 28c3

Researchers were able to identify devices against plots sent to Discovergy servers

Pent Hertz

Smart meters architectures



Source: https://www.mouser.com/pdfdocs/Solar-Maxim-Smart_Grid_Communications.pdf

Smart meters protocols

Region	WAN	NAN	HAN
North America	Cellular, WiMAX	G3-PLC, HomePlug®, IEEE 802.15.4g, IEEE P1901, ITU-T G.hnem, proprietary wireless, Wi-Fi	G3-PLC, HomePlug, ITU-T G.hn, Wi-Fi, ZigBee, Z-Wave
Europe	Cellular	G3-PLC, IEEE P1901, ITU-T G.hnem, PRIME, Wi-Fi	G3-PLC, HomePlug, ITU-T G.hn, Wi-Fi, Wireless M-Bus, ZigBee
China	Cellular, band-translated WiMAX	G3-PLC, RS-485, wireless to be determined	G3-PLC, RS-485, Wi-Fi, to be determined
Rest of the World	Cellular, WiMAX	G3-PLC, HomePlug, IEEE 802.15.4g, IEEE P1901, ITU-T G.hnem, PRIME, RS-485, Wi-Fi	G3-PLC, HomePlug, ITU-T G.hn, RS-485, Wi-Fi, Wireless M-Bus, ZigBee, Z-Wave

Source: https://www.mouser.com/pdfdocs/Solar-Maxim-Smart_Grid_Communications.pdf

Do you see something familiar here?

Smart meters protocols

Region	WAN	NAN	HAN
North America	Cellular, WiMAX	G3-PLC, HomePlug®, IEEE 802.15.4g, IEEE P1901, ITU-T G.hnem, proprietary wireless, Wi-Fi	G3-PLC, HomePlug, ITU-T G.hn, Wi-Fi, ZigBee, Z-Wave
Europe	Cellular	G3-PLC, IEEE P1901, ITU-T G.hnem, PRIME, Wi-Fi	G3-PLC, HomePlug, ITU-T G.hn, Wi-Fi, Wireless M-Bus, ZigBee
China	Cellular, band-translated WiMAX	G3-PLC, RS-485, wireless to be determined	G3-PLC, RS-485, Wi-Fi, to be determined
Rest of the World	Cellular, WiMAX	G3-PLC, HomePlug, IEEE 802.15.4g, IEEE P1901, ITU-T G.hnem, PRIME, RS-485, Wi-Fi	G3-PLC, HomePlug, ITU-T G.hn, RS-485, Wi-Fi, Wireless M-Bus, ZigBee, Z-Wave

Source: https://www.mouser.com/pdfdocs/Solar-Maxim-Smart_Grid_Communications.pdf

Do you see something familiar here? → use of PLC and HomePlug

Renewable energy storage

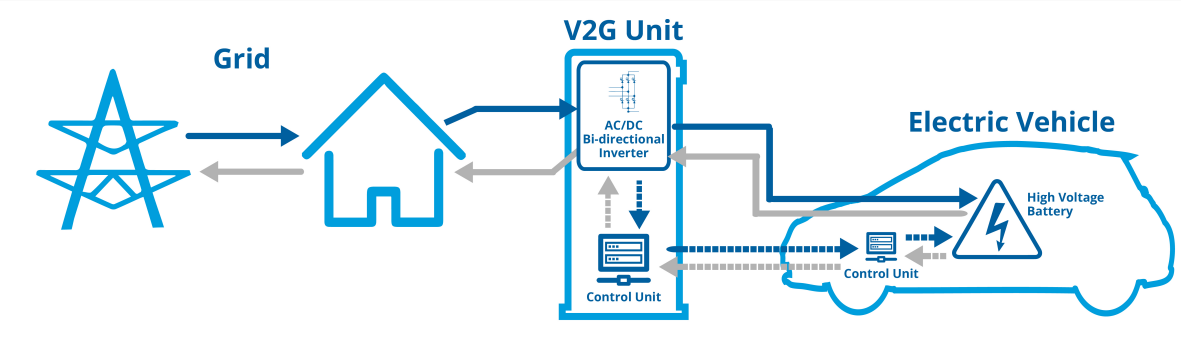
Long story short: renewable energy

- Renewable energy production → variable and difficult to predict (solar, wind, user consumption, etc.)
- People had to think about ways to store it
- First energy storage system → Battery-to-Grid (B2G)
- In // Electric Vehicles → gaining popularity (U.S.A., Japon, China and UE)

→ Why not use car's battery for energy storage too?

The rise of V2G

- V2G: Vehicle-to-Grid
- Use Electric Vehicles (EVs) to store energy
- In bidirectional charging/discharging systems → pay for charging or get paid → compensate battery deterioration



source: automobile-propre.com

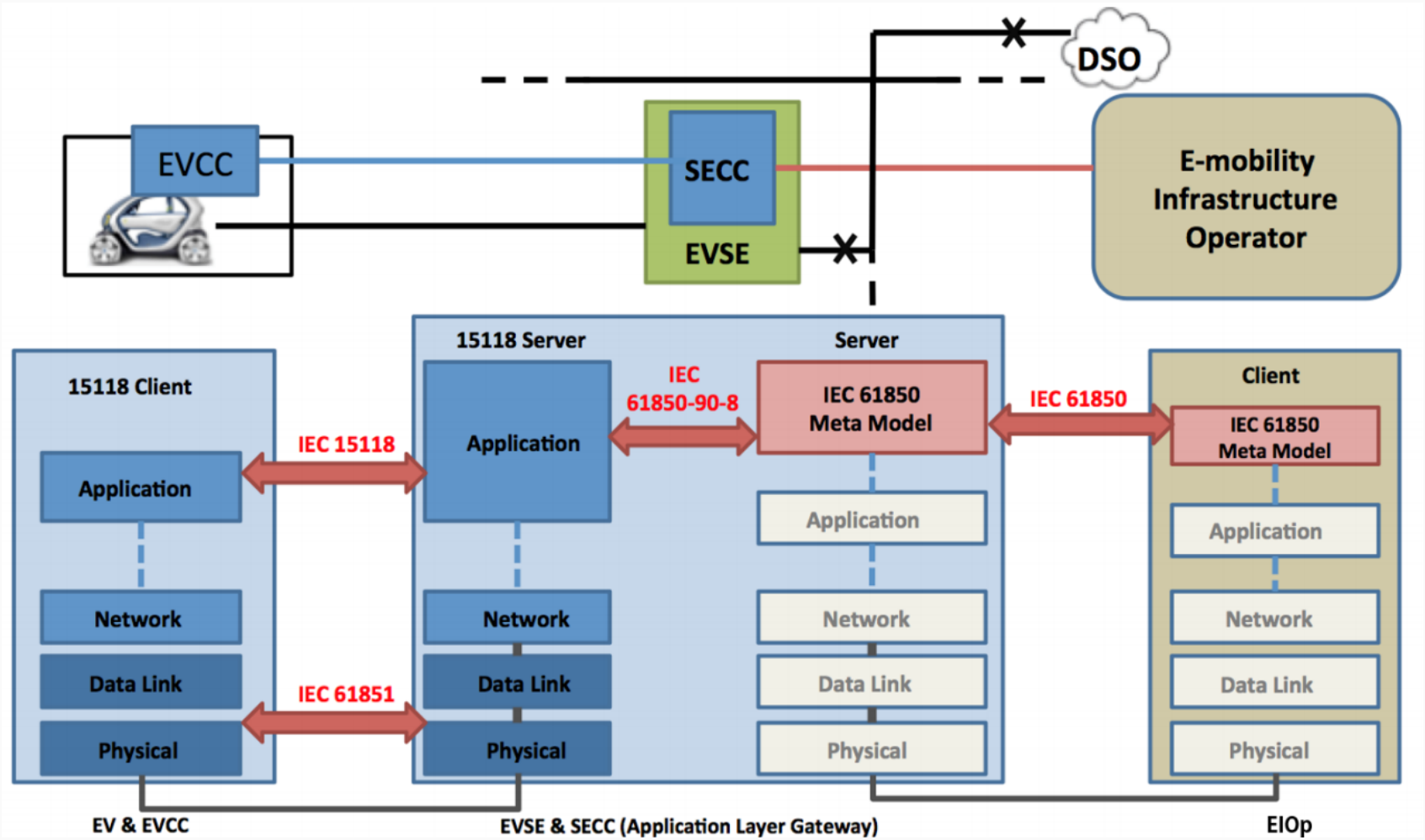
Looking at specs → V2G systems communicate with a protocol

Standards for interoperability

V2G uses several standards to communicate:

- ISO/IEC 15118: Vehicle-to-Grid (V2G) communication
- IEC 61851: conductive charging system
- IEC 61850-90-8: communication networks for EVs
- and so on.

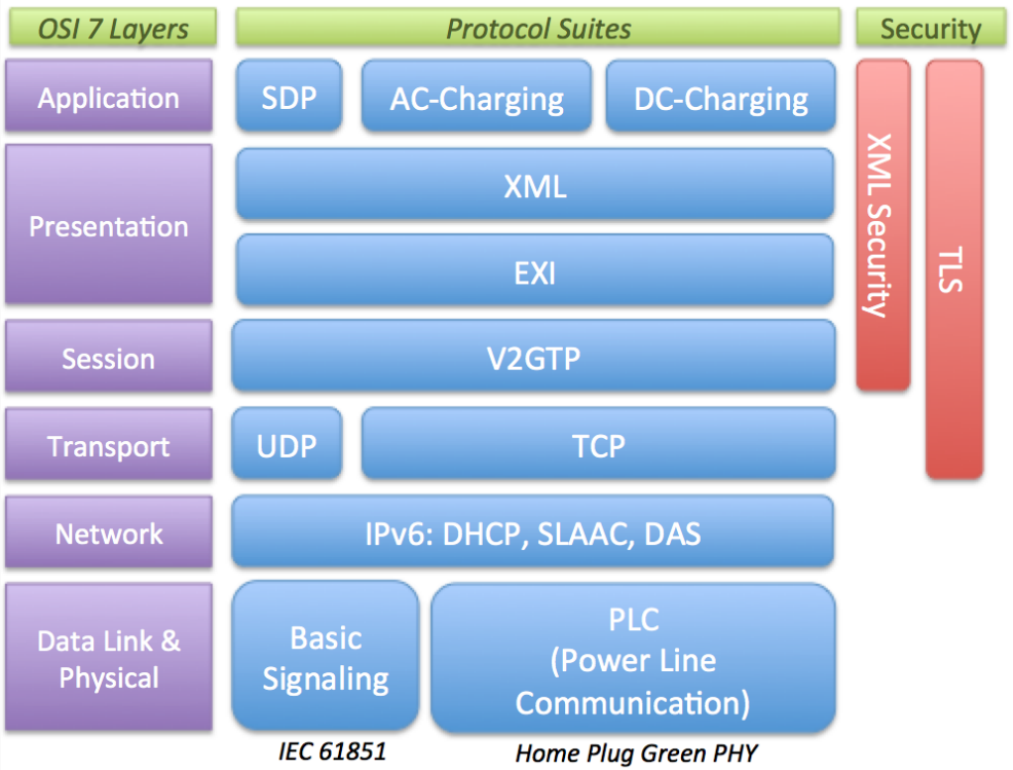
Architecture



source: https://res.mdpi.com/applsci/applsci-06- 00165/article_deploy/applsci-06-00165.pdf

V2G layers

- V2G data exchanged over IPv6
- SECC (UDP) → EV Supply Equipment (EVSE) host and port
- XML data → EXI encoded
- HomePlug Green PHY used to transfer data...



source: https://res.mdpi.com/applsci/applsci-06-00165/article_deploy/applsci-06-00165.pdf

HomePlug PLC devices

Introduction

- PLC: Powerline Communication
- Principle discovered by Edward Davy in 1838
- Released in the early 2000s for home applications
- Evolves a lot in therms of speed

Could be found in various applications.

Applications

Classical: domestic

- Use HomePlug specifications (Ex. HomePlug AV)
- Extend a local network
- Depending on the context cheaper than buying multiple repeaters
- Generally more reliable than Wi-Fi

Other cases

Applications

Classical: domestic

Other cases

- Electrical counters:
  - Like Cenélec (3-148.5 kHz low voltage) are used : meter readings, intruder alarms, fire detection, gaz leak detection, and so on.
  - Linky G3, G1 specs, etc.
  - But some countries use HomePlug specifications for their counters
- Smart grid $\rightarrow$ recently found in missions
- Home automation
- And so on.

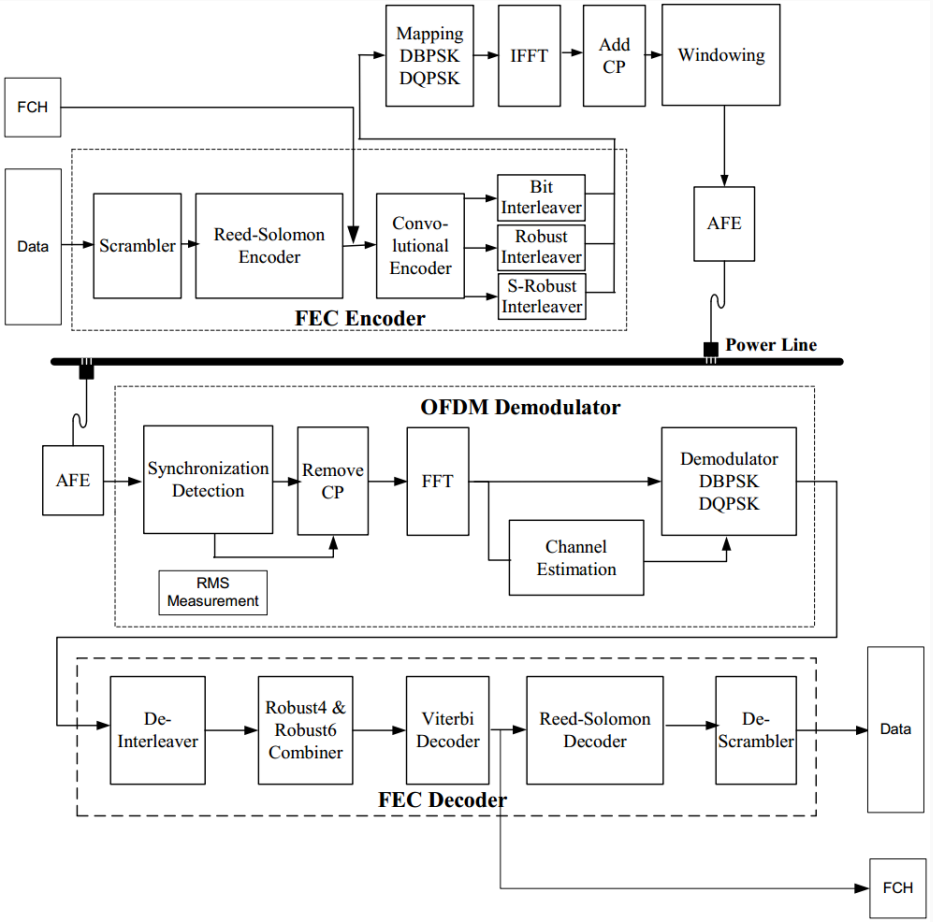
Data propagation: reminders

- AC voltage is 50 Hz $\rightarrow$ a signal do 50 cycles/s
- Could be represented by the formula: $Ps = A\sqrt{2}sin(2\pi ft)$ (f: frequency in Hz; t: time)
- The data (Da) is superposed to this carrier $\rightarrow$ $Td = Ps + da$)

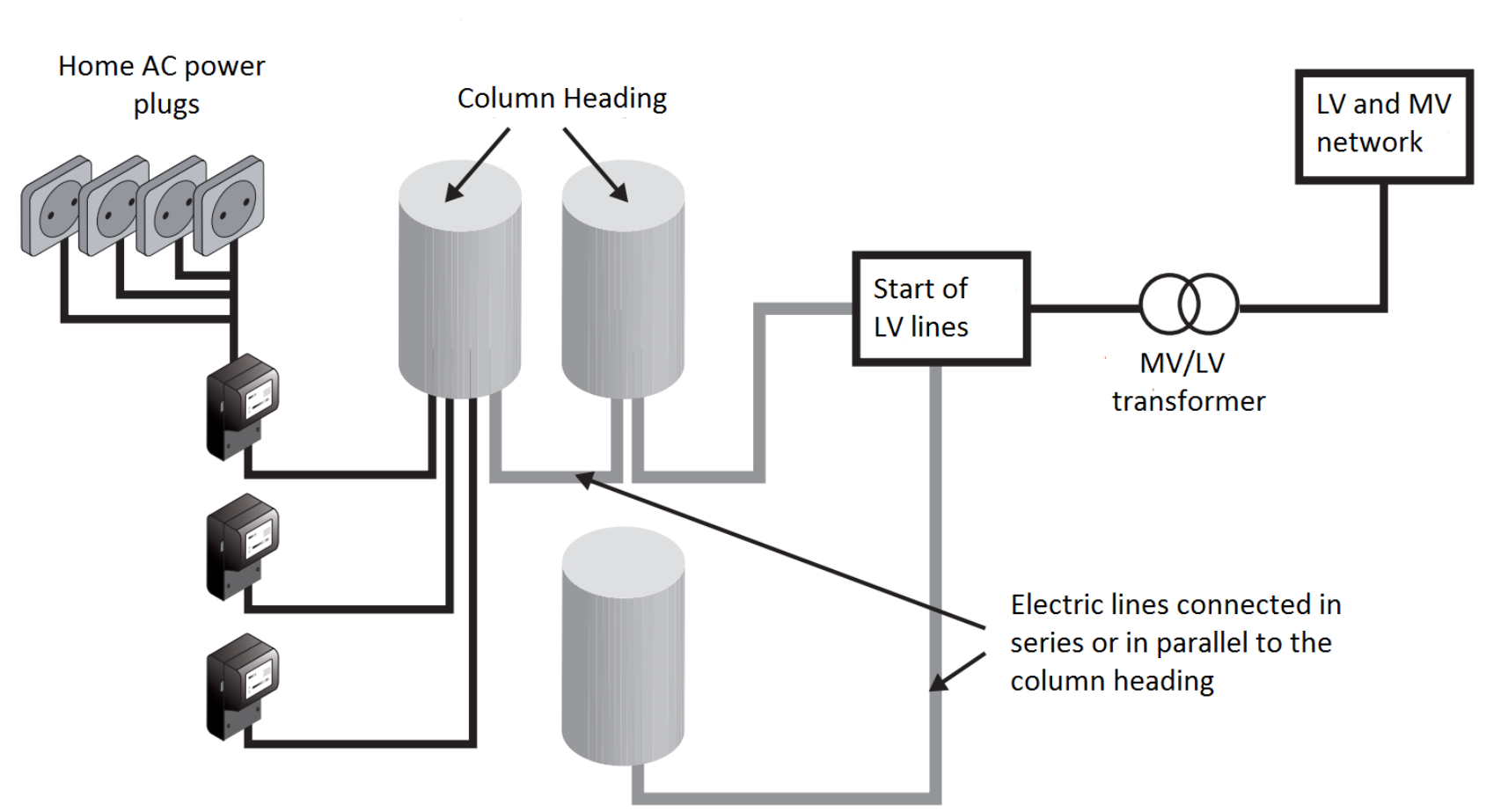
But before being sum to the power supply $\rightarrow$ need error detection, code mapping, multi-carrier modulation

Data propagation: DSP

1. data scrambling
2. turbo encoding
3. modulation of control and data frames
4. form OFDM symbols
5. windowing
6. etc.

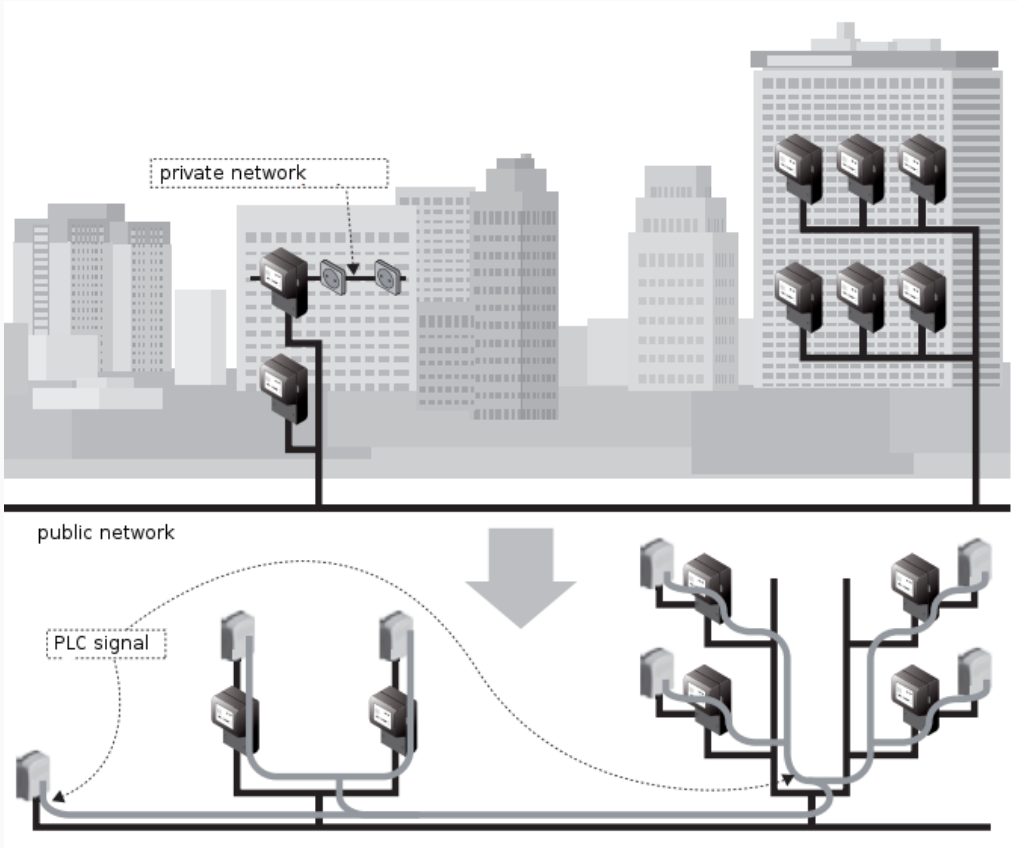


Data transmission at home



source: PLC in Practice by Xavier Carcelle

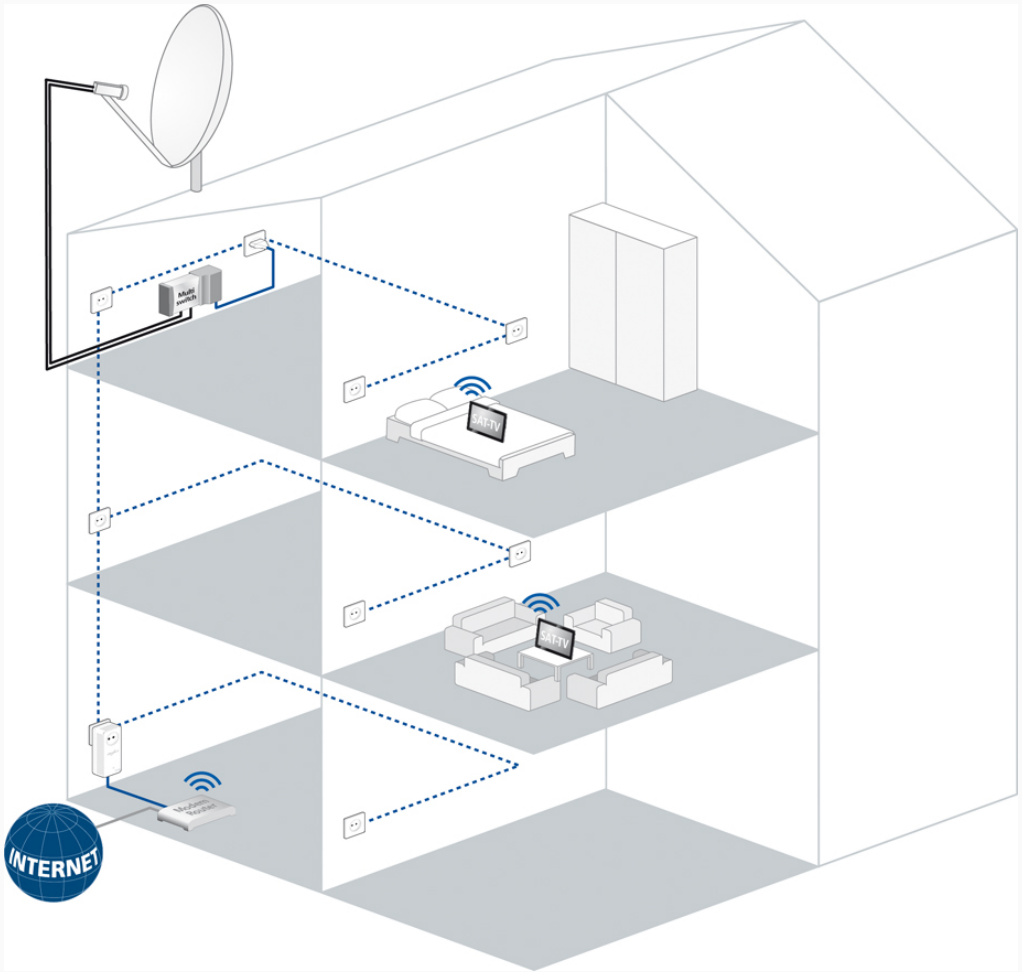
Private vs Public network



source: PLC in Practice by Xavier Carcelle

- In reality: no choc-coil → no real private network

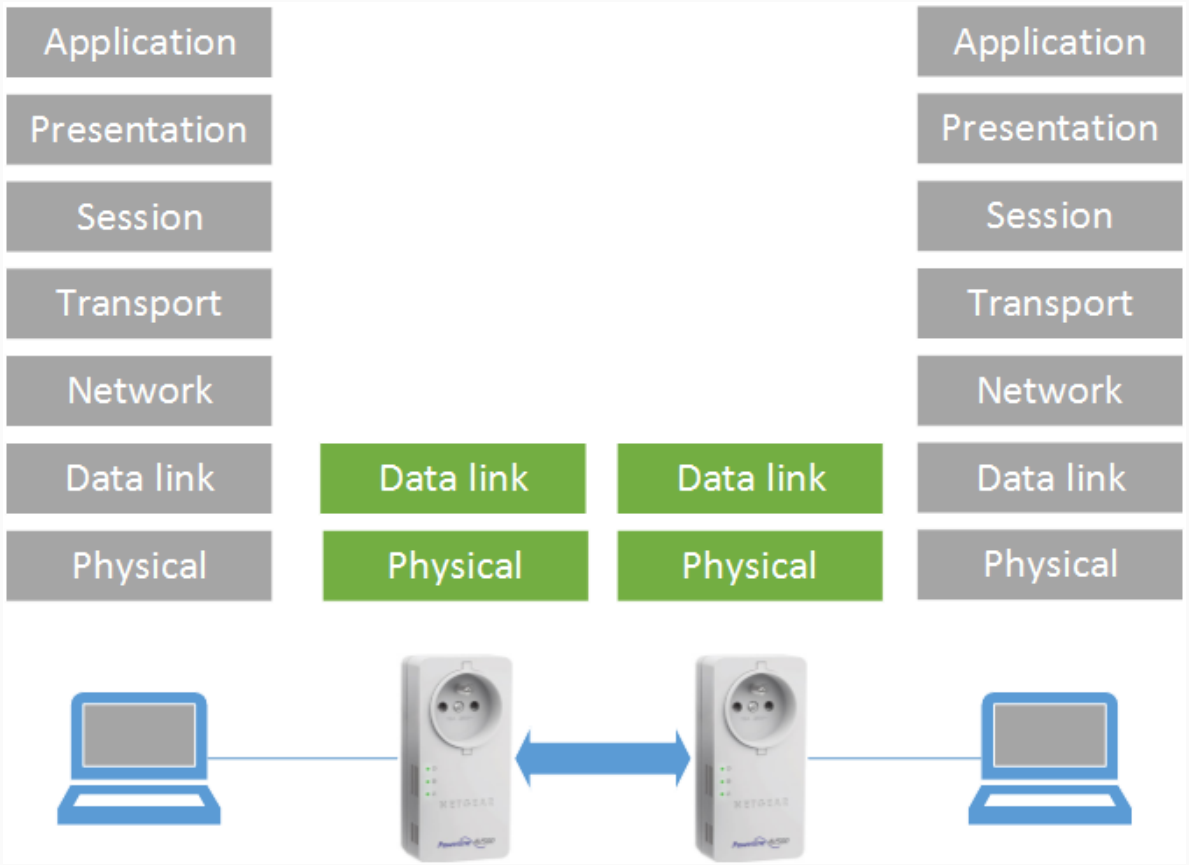
Data transmission at home



source: Devolo

PLC layers

A PLC uses layer 1 and 2 of the OSI model → IEEE 802.3



Communications

Computer ↔ PLC

- Communicate through Ethernet on MAC layer
- Clear text (no ciphering)

PLC ↔ PLC

- Communicate through powerline
- Data is encrypted (using AES CBC 128 bits on new PLCs)

Everything is defined in HomePlug AV specifications

Interroperability

		CPL A	CPL B					
			HomePlug				DS2	Spidcom
			1.0, Turbo	AV	Oxance	BPL	CC	
HomePlug	1.0, Turbo							
	AV							
	Oxance							
	BPL							
	CC							
DS2 AV200								
Spidcom								

But also with HomePlug Green PHY

HomePlug AV and GP

Homeplug GP (Green PHY) → subset of HomePlug AV

HomePlug GP PHY Simplifications Reduce Cost & Power Consumption

	Parameter	HomePlug AV	HomePlug GP
PHY	**Spectrum**	2 MHz to 30 MHz	2 MHz to 30 MHz
	Modulation	OFDM	OFDM
	# Subcarriers	1155	1155
	Subcarrier spacing	24.414 kHz	24.414 kHz
	Supported subcarrier modulation formats	BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM, 1024 QAM	QPSK only
	Data FEC	**Turbo code** Rate ½ or Rate 16/21 (punctured)	**Turbo code** Rate ½ only
	Supported data rates	**ROBO:** 4 Mbps to 10 Mbps **Adaptive Bit Loading:** 20 Mbps to 200 Mbps	**ROBO:** 4 Mbps to 10 Mbps

HomePlug AV and Green PHY

- HomePlug Green PHY (HPGP) $\rightarrow$ subset of HomePlug AV
- HomePlug AV used to extend domestic local network
- HPGP Intended to be used for ”smart” grid or other automation systems
- Throughput decreased $\rightarrow$ use of QPSK instead of high order QAM
- HomePlug AV higher peak rate than HomePlug Green PHY

Publication

- Power Line Communications in Practice by Xavier Carcelle → a must read!
- HomePlug AV Security Mechanisms by Richard Newman, Larry Younge, Sherman Gavette, and Ross Anderson, published in 2007
- MISC #37 HomePlug Security by Xavier Carcelle
- HomePlugAV PLC: Practical attacks and backdooring, at NoSuchCon 2014, by Sébastien Dudek → introducing a flaw in Direct Access Key (DAK) generation
- V2G Injector: Whispering to cars and charging units through the Power-Line, at SSTIC 2019, by Sébastien Dudek → introducing a new flaw in HomePlug Green PHY

Tools

- plconfig → manage PLCs over the network
- FAIFA[2] by Xavier Carcelle (similar to plconfig) → first Open source PLC tool
- Vendors' softwares
- open-plc-utils[3] by Qualcomm Atheros, published after FAIFA
- Wireshark has a dissector for HomePlugAV, but not for HomePlug GP
- HomePlugPWN[4] by Sébastien Dudek: Scapy dissectors for HomePlug AV / GP**(new)**, attack DAK keys and collect HomePlug GP secrets**(new)**

[2] https://github.com/ffainelli/faifa
[3] https://github.com/qca/open-plc-utils
[4] https://github.com/FlUxIuS/HomePlugPWN

An accessible technology

- Used for domestic purposes
- Some tools are also accessible
- Same technology is used for Smart grid devices → and everything is spread on an electrical line...

Current attacks

Identification of devices

2 techniques:

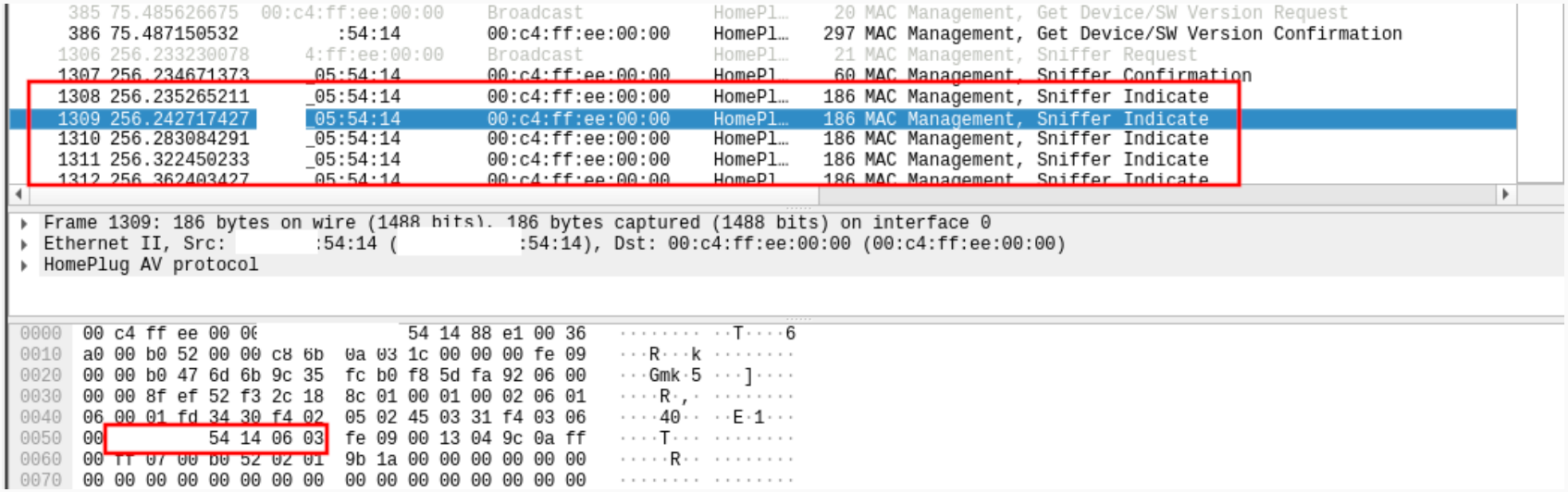
1. NetworkInfo Req $\rightarrow$ Confirmations $\rightarrow$ Station informations
2. Enable Sniff Mode $\rightarrow$ get MME of Central Coordinators (CCo)
    - A detected CCo = potential AV logical network

But *NetworkInfo* confirmation messages list stations of the same AVLN only $\rightarrow$ need to be smarter

Detection of HomePlug AV/GP devices with sniff mode

To detect Central Coordinator (CCo) devices → same old tricks are still possible:

1. Enabling sniff mode with *plcmon.py* provided in HomePlugPWN tool
2. See all EVSE that appears as CCo devices reported by Sniff indicate packets



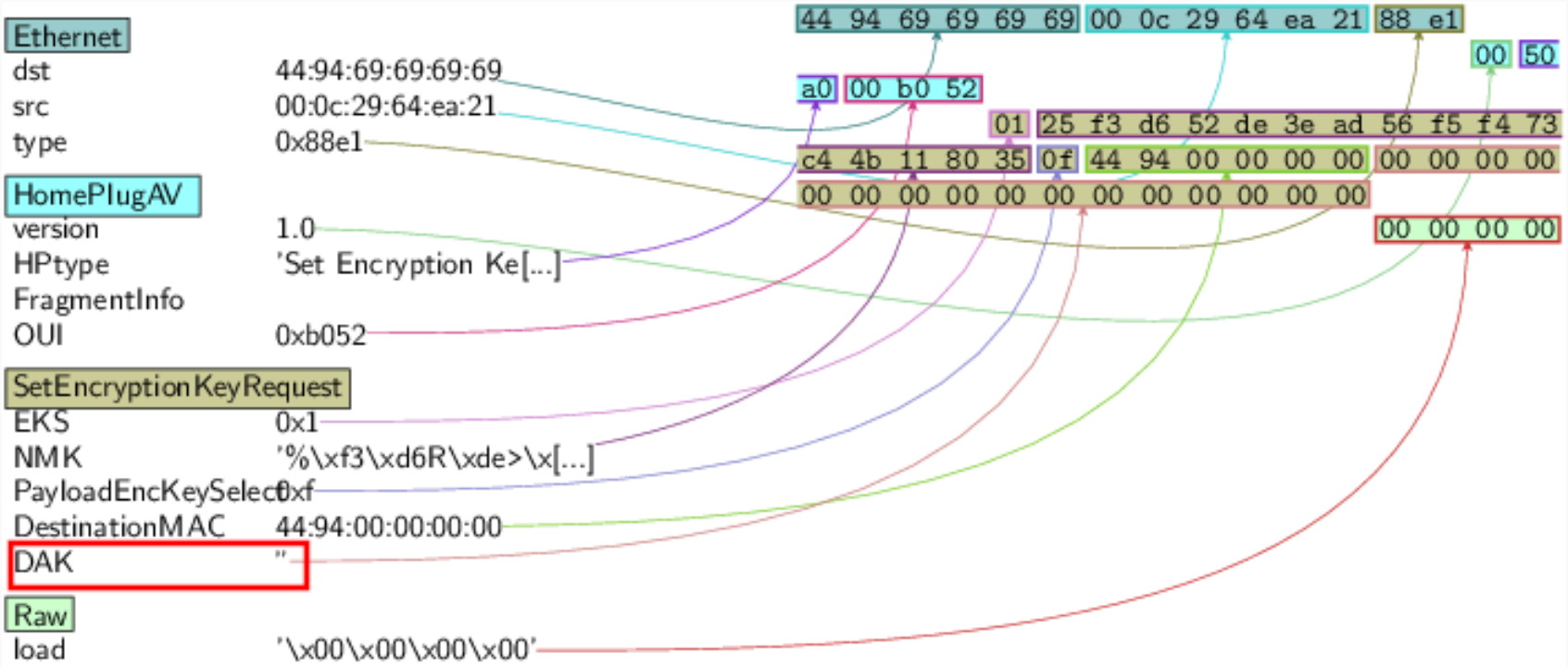
HomePlug AV and Green PHY keys

2 kinds of keys to manage and encrypt data:

- Network Membership Key (NMK): to encrypt the communication using 128-bit AES CBC
- Direct Access Key (DAK): to remotely configure the NMK of a targeted PLC device over the Power-Line interface

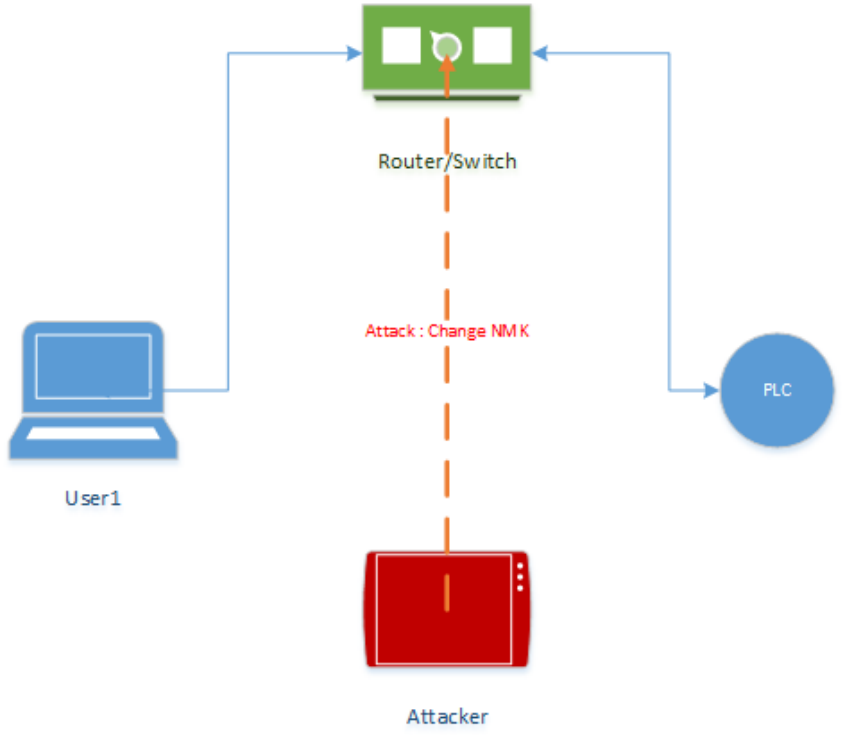
Configuring the NMK

- if local → DAK can be empty
- remotely the DAK of the targeted device should be included



Attacking the local/management interface

- Ethernet interface: allowed to perform privileged operations
- If an attacker is on the LAN $\rightarrow$ backdoor the device:
  - Program it's own NMK
  - Replace device's firmware



DAK generation status

- Qualcomm devices had a weak DAK → see our research paper presented at NSC 2014
- In Feb 2015: Qualcomm patched their utility, refering to their GitHub:

```
@@ -183,25 +190,28 @@ static void function (const char * file, unsigned count, unsigned group, unsigne
 *                                                                    */

-#define DEFAULT_COUNT 25
-#define DEFAULT_GROUP 5

 int main (int argc, const char * argv [])

 {
+       extern void (* passwords)(unsigned, unsigned, unsigned, unsigned, unsigned, char, flag_t);
        static const char * optv [] =
        {
-               "b:l:qs:uv",
+               "b:l:mqs:rv",
                PUTOPTV_S_FUNNEL,
                "Atheros device password generator",
-               "b n\tbunching factor [" LITERAL (DEFAULT_GROUP) "]",
-               "l n\tpassword letters [" LITERAL (DEFAULT_COUNT) "]",
+               "b n\tbunching factor [" LITERAL (DEFAULT_BUNCH) "]",
+               "e\tbase password on host system entropy",
+               "l n\tpassword letters [" LITERAL (DEFAULT_ALPHA) "]",
+               "m\tbase password on MAC address (less secure)",
```

But still devices from 2015 and older + chineese and some other devices remain vulnerable

Attacking vulnerable devices

- Discover CCo to get a MAC address:

```
python plcmon.py
[+] Enabling sniff mode
Sent 1 packets.
[+] Listening for CCo station...
         Found CCo: 44:94:fc:56:ff:34 (DAK: RMHT-ILPO-TYMN-IIXY)
         [...]
```

- Run K.O.DAK attack to reconfigure the NMK remotely:

```
python quickKODAK.py -i eth0 -t 4494fc56ff34
Sent 1 packets.
```

- Configure our PLC to connect to the targeted AVLN

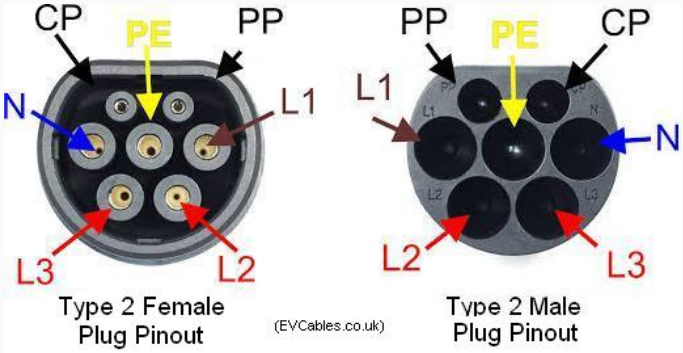
Intruding V2G networks

Starting vector

The Combined Charging System connectors

Different types of connectors exist, like IEC 62196 in UE:

- PP: Proximity pilot for pre-insertion signaling
- CP: Control Pilot for post-insertion signaling
- PE: Protective earth
- N: Neutral (single/3 phase AC/DC-mid)
- L1, L2 and L3 three-phase AC/DC-mid



HGPG data multiplexed onto the Control Pilot and ground lines

Our first device to test it

dLAN Green PHY eval board EU II → multiple interfaces

But cheaper alternatives exist

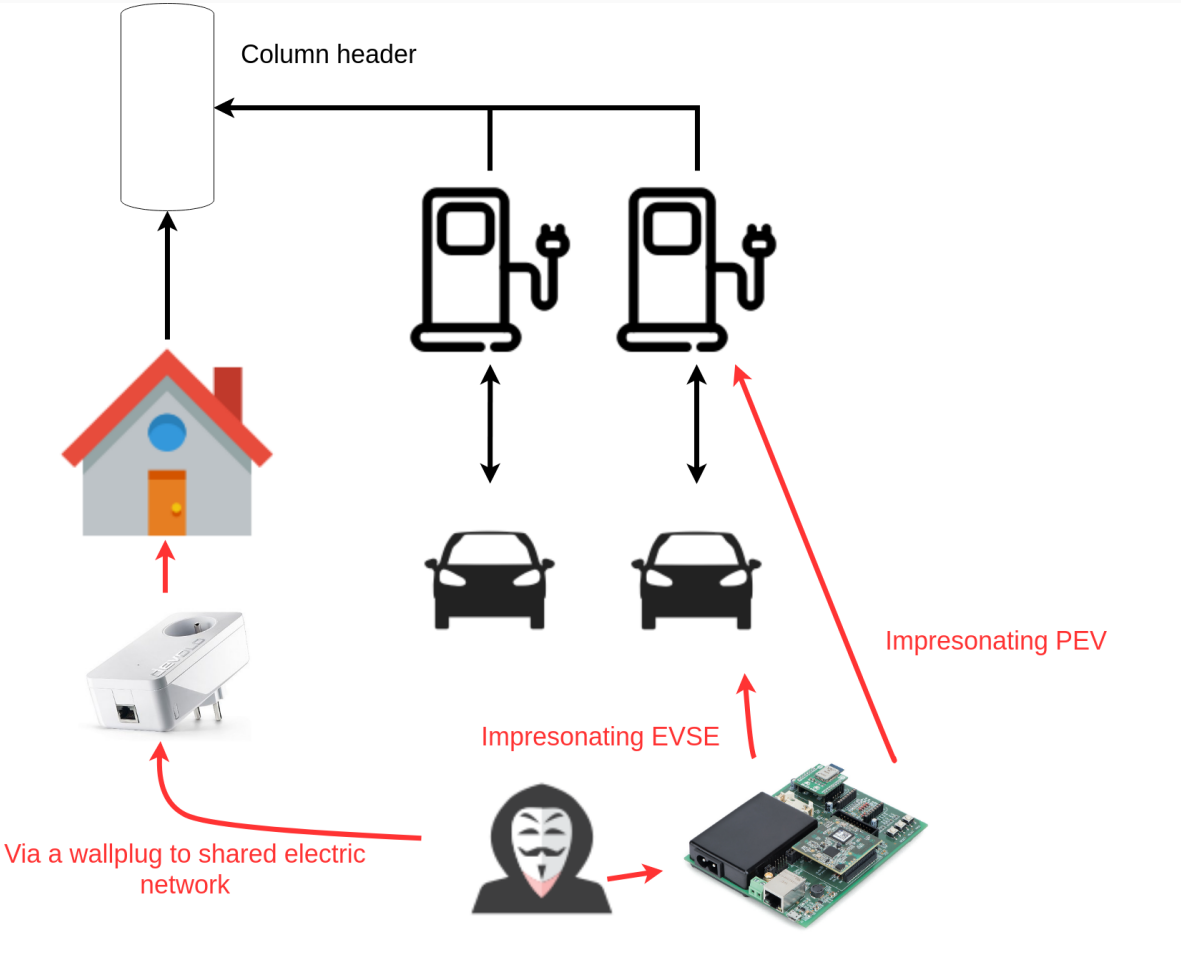
Cheapest way: the wallplug

- Any QCA 7k will do the work
- Ex: Devolo 1200+ works like a charm
- No modification needed if charging stations share the same electrical network
- Otherwise, some rework should be done on the coupler

We are actually working on some modular rework with this adaptor

Pent Hertz

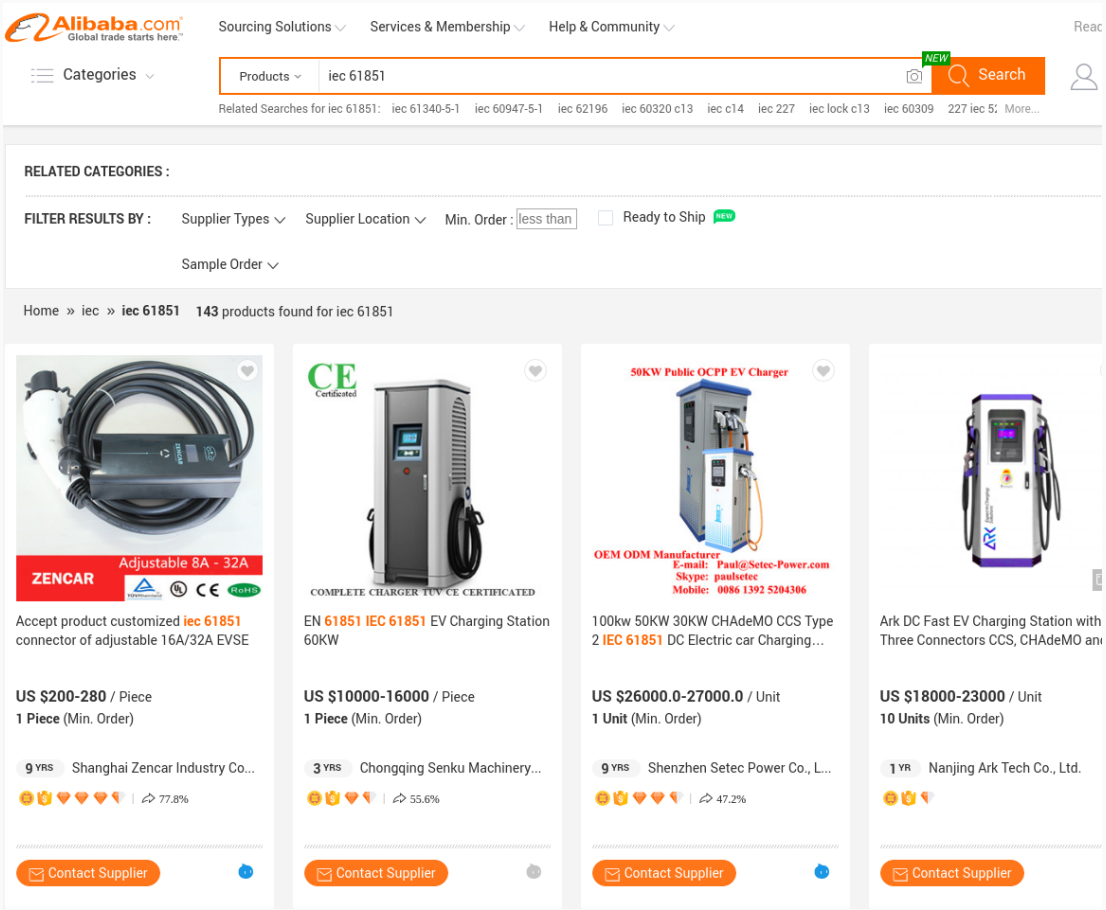
How to interface



With a charging station connector

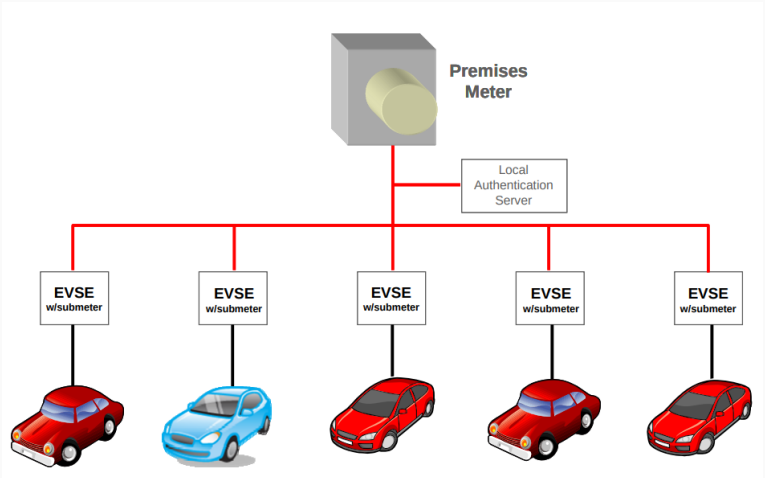
Where can we find those connectors?

You can really find everything in Alibaba, even charging stations...



Plug-in Electrical Vehicle (PEV) Association

- PEV can be charged everywhere (public, home, etc.)
- It leaves unconfigured in new AVLN (AV Logical Network)
- So it needs to join the AVLN of the corresponding EVSE once plugged with a charging connector



source: HomePlug Green PHY whitepaper

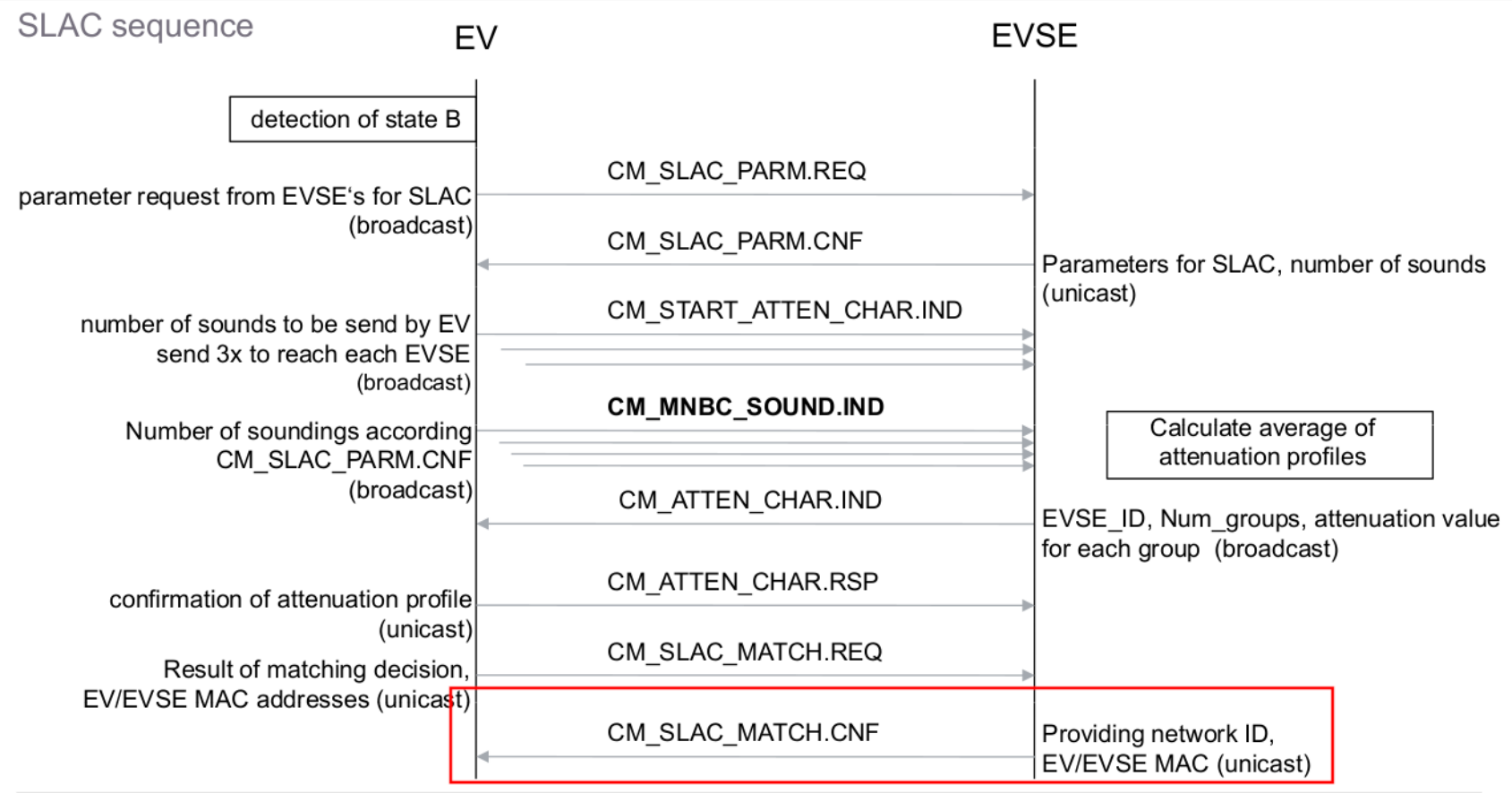
Use of SLAC procedure

Pent Hertz

SLAC procedure

- SLAC: Signal Level Attenuation Characterization
- Aimed to avoid bad association (avoid billing errors, etc)
- Principle:
  1. PEV broadcast unacknowledged SOUNDING packets
  2. Stations (EVSE) around measure the received power and send it to the PEV
  3. PEV finally select the EVSE with the best result
  4. Then EVSE provides a network (how???)

SLAC procedure (2)



source: HomePlug Green PHY whitepaper

HomePlug Green PHY modes

Can be set in 3 specific modes:

- Unconfigured
- PEV: can see HPGP specific packets from EVSE
- EVSE: see HGPG specific packets from PEV

Each mode allows or disallows the interception of certain HomePlug GP packets at MAC Layer 2

HomePlug Green PHY modes

Can be set in 3 specific modes:

- Unconfigured
- PEV: can see HPGP specific packets from EVSE
- EVSE: see HGPG specific packets from PEV

Each mode allows or disallows the interception of certain HomePlug GP packets at MAC Layer 2

Warning

Need the correct mode to collect MME packets of a specific device

Changing SLAC mode

Change SLAC mode into PEV modifying byte 0x1653 with "setpib" after dumping it with *plctool*[5]:

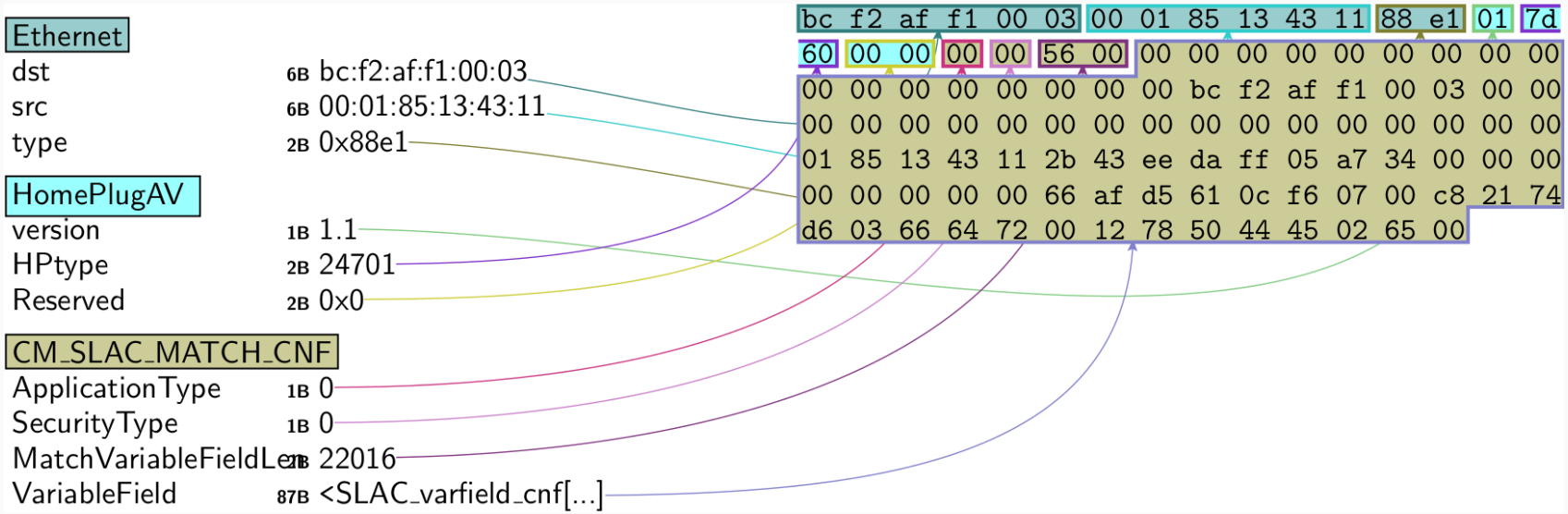
```
$ setpib PIBdump.pib 1653 byte 1
```

Then → capture packets coming from EVSEs

[5] https://github.com/qca/open-plc-utils

A flaw in the SLAC procedure

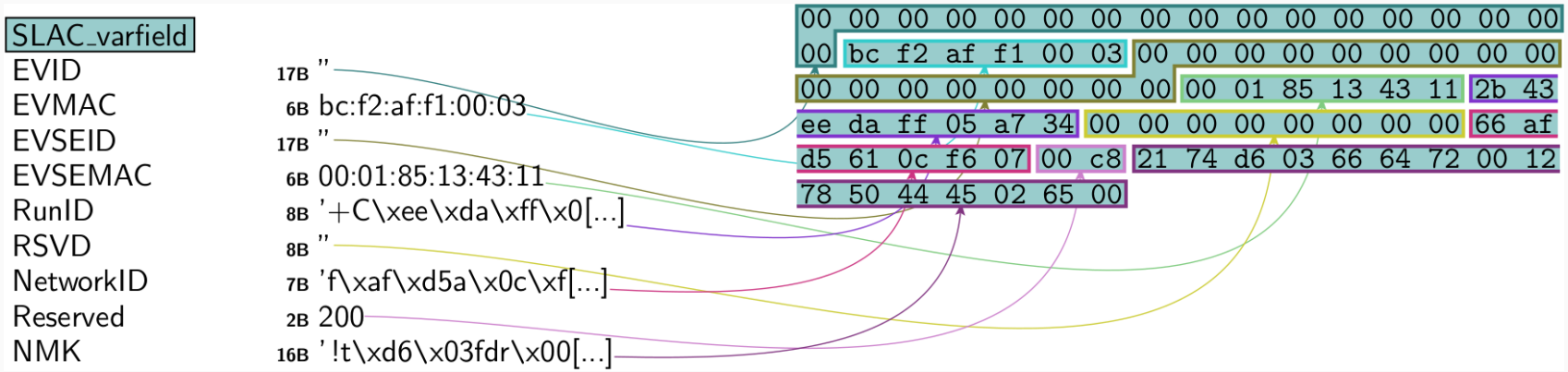
When analyzing the SLAC procedure → surprise!



It was supposed to be a unicast packet, isn't it? → but it is broadcasted in the Power-Line!

Getting keys of AVLNs

By decoding the different fields of the *CM_SLAC_MATCH.CNF* message:



Our PLC can be easily set by changing “slac/pev.ini” profile and used with “pev” tool[6]

[6] https://github.com/qca/open-plc-utils

Into the AVLN

- Once part of an AVLN $\rightarrow$ we can talk to every possible device into the same AVLN
- Reach services exposed by devices
- Intercept exchanged data EV $\leftrightarrow$ charging station

More about: V2G Injector

- Available: https://github.com/FlUxIuS/V2GInjector
- Paper, slides and recording: click here (SSTIC 2019)

Attacking the charging station

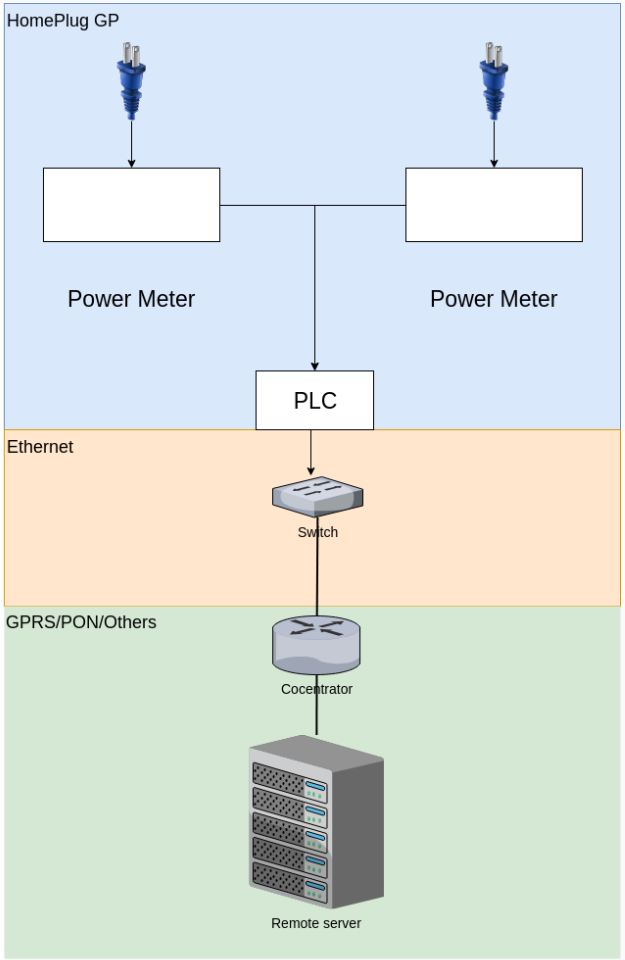
- Runs a complex OS (Linux generally)
- Some available services:
  - V2G webservice
  - SSH
  - Web console/management/log interface
  - Sometimes: Telnet and more...
- Connected to an operator
- If attacked → used as pivot

Pent Hertz

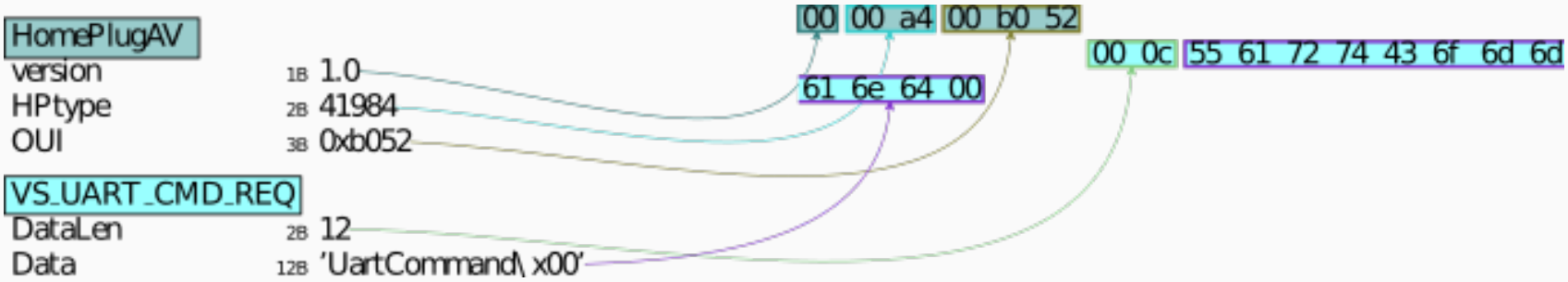
Intruding from smart meters

HomePlug applied to Smart Grids

- HomePlug SG (Smart Grids) → subset of HomePlug GP
- A master (CCo) PLC is connected to a switch
- Each power meter use a PLC modem to connect to a CCo PLC
- Sends UART commands through PowerLine → WTF?!



Very simple to generate with Scapy



- You can test it on detected devices → it will reply with a confirmation message
- Implemented in HomePlugPWN[7]

[7] https://github.com/FlUxIuS/HomePlugPWN/blob/master/layerscapy/HomePlugSG.py

Smart cities = UART cmds everywhere?!

But you know...

Get the NMK key

- An AVLN can hold 254 stations max.
- Each node instantiated by a CCo $\rightarrow$ different NMK
- And we need to get this NMK somehow...

This secret is stored somewhere...

Program Information Blocks (PIB)

- Used to store PLC's configuration
- Enables/Disables certain modes (WireTap, Sniffing, SLAC, etc.)
- A lot of non-documented blocks
- Many features could be discovered by digging this way

A lot of blocks have been retrieved and implemented in *ModulePIB*[8] of the *HomePlugAV.py* Scapy layer → still needs more work to decode all of them

[8] `https://github.com/FlUxIuS/HomePlugPWN/blob/master/layerscapy/HomePlugAV.py`

Dump PIB

2 tools:

- *PIBdump.py* of *HomePlugPWN*
- *plctool* of *open-plc-utils* → support more PLC chipsets

```
./plctool -f -i enp0s31f6 -p /tmp/plc.pib local
enp0s31f6 00:B0:52:00:00:01 Fetch NVRAM Configuration
enp0s31f6 F4:06:8D:CE:00:7D TYPE=0x15 (M25P32_ES) PAGE=0x0100 (256) BLOCK=0x10000
 (65536) SIZE=0x400000 (4194304)
enp0s31f6 00:B0:52:00:00:01 Read Module from Memory
```

Management interface only

Only work on the management interface, and not directly on the PLC interface. Unless you have a DAK key.

Analyze PIB

The tool *chkpib* of *open-plc-utils* allows extracting information:

- *PIBdump.py* of *HomePlugPWN*
- *plctool* of *open-plc-utils* → support more PLC chipsets

```
./chkpib -mv /tmp/plc.pib
------- /tmp/plc.pib (0) -------
        [...]
------- /tmp/plc.pib -------
        PIB 0-0 19928 bytes
        MAC F4:06:8D:CE:00:7D
        DAK A7:6B:****************************************
        NMK 36:34:C5:DF:2E:6E:4F:7D:72:05:F5:8D:39:29:53:C0
        NID 96:46:60:59:BF:F8:05
        Security level 0
        NET
        MFG Delta Electronics Mon 27 May 2019 06:05:29 PM CEST
        USR Qualcomm Atheros Enabled PEV
        CCo Never
        MDU N/A
```

With the NMK

- We are able to intrude the network from Smart grid device like a Smart Meter
- Whats is next? $\rightarrow$ depends on the operators
- We can be tempted to:
  - Scan and discover other devices or hosts
  - Hunt for vulnerability in exposed devices or hosts
  - Etc.

Conclusion

Conclusion

- Power-Line Communication is almost everywhere
- HomePlug is widely used, accessible and some attacks can be engaged
- Logical vulnerabilities exist in specs and vendors configurations
- A lot of bugs under the Layer 2 MAC could be found $\rightarrow$ but PLC is not open enough (we're working on it)
- Much more work should be also done on ITU-T G.hn $\rightarrow$ widely used in NAN as in HAN
- G3-PLC and PRIME are not publicly explored yet, but are less accessible

Questions?

Thanks!


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
BOLZÏN
MERCI
BÏYAN
SHUKRIA
DANKSCHEEN
TASHAKKUR ATU
YAQHANYELAY
SUKSAMA
EKHMET
MEHRBANI
GRAZIE
MAAKE
KOMAPSUMNIDA
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
PALDIES
TINGKI
SPASSIBO
SNACHALHUYA
NUHUN
CHALTU
WABEEJA
MAITEKA
YUSPAGABÀTAM
HUI
DHANYABAAD
ANIHA
ATTO
LAH
SANCO
MERASTAWHY
GAEJTHO
AGUYJE
FAKAAUE
TAVTAPUCH
MEDAWAGSE
BANYA
GU
HATUR
EKOJU
SIKOMO
MAKETAJ
MINMONCHAR
SPASIBO
DENKAUJA
NENACHALHYA
UNALCHÉESH
MERSI