École Polytechnique Fédérale de Lausanne
University of Oxford

Evaluating the Scale and Attack Surface of PLC Deployments

by Isis Beloslava Daudé

Master Thesis

Approved by the Examining Committee:

Dr Sebastian Köhler
Thesis Supervisor - University of Oxford

Prof. Ivan Martinovic
Thesis Advisor - University of Oxford

Prof. Dr. sc. ETH Mathias Payer
Thesis Advisor - EPFL

EPFL IC IINFCOM HEXHIVE
BC 160 (Bâtiment BC)
Station 14
CH-1015 Lausanne

March 8th, 2024

Opportunities multiply as they are seized.
— Sun Tzu
Hakuna Matata
— Lion King

Dedicated to Guergana and Colin.

Acknowledgments

I would like to express my warmest gratitude to the SSL team, for welcoming me and allowing me to work with them. In particular, I would like to thank Dr Sebastian Köhler for his considerate supervision and support, as well as Prof. Ivan Martinovic for advising my thesis. Their insights, constant feedback, and expertise have been invaluable in shaping the research direction and improving the quality of my work. I would also like to give my special thanks to members of the lab with which I enjoyed working: Simon, Josh, Edd and Marcell.

I would like to express my sincerest gratitude to my EPFL advisor, Prof. Dr. sc. ETH Mathias Payer, for his guidance throughout the course of my thesis and for giving me advice when in need. I would also like to acknowledge the use of this LaTeX template, which he kindly provided as open-source.

I would like to mention all my friends who have supported me throughout my academic journey, whether in Lausanne, Milan, Zurich or Oxford. I am grateful and infinitely lucky to have had amazing people surrounding me with love and appreciation all these years.

Farida, Thank you for your support, love and letting me borrow your strength when mine was lacking. I love you.

Last but not least, I would like to thank my family with all my heart for always being by my side. I cannot express in words the amount of love I feel for you, and how I am grateful for having you in my life.

Merci mon Papa de m'avoir soutenue quand j'en avais besoin. Je t'aime.

Благодаря ти, че винаги си до мен и се бориш за мен. Обичам те, мамо.

(*Thank you for always being by my side and fighting for me. I love you Mamo*)

Lausanne, March 8, 2024 Isis Beloslava Daudé

Abstract

Power-Line Communication (PLC) is increasingly popular as an alternative to WiFi allowing devices to connect to the Internet without the installation of new wires. In particular, the HomePlugAV standard, which promises speeds similar to Ethernet cabling, has become well-known. However, over the years, numerous attacks against PLC devices have been discovered. These attacks grant full access to the victim network, leading to severe consequences.

While, historically, these attacks have required physical access to the power lines, we show that this requirement is no longer necessary. We demonstrate that due to the strong electromagnetic leakage of PLC, these vulnerabilities can be exploited wirelessly using only off-the-shelf equipment. We perform an extensive evaluation in a laboratory environment and in real-world deployments to understand the possibilities, requirements, and limitations of a wireless attacker. In our real-world experiments, we found that an off-the-shelf PLC modem, without any modifications and without additional amplification, is sufficient for an adversary to wirelessly join a PLC network from a distance of up to 1.5 m from the target building and interact with other devices. Eavesdropping on the communication can be achieved with a larger distance, up to 4 m away from the target building. Our results show that the perceived security of limited physical access to power lines is false, and that an adversary can indeed access the network wirelessly.

Contents

Chapter 1

Introduction

With a growing need for efficient data transmission and multimedia communications, Power-Line Communication (PLC) technologies have seen rapid adoption over the last decades. Thanks to the ability of PLC to use existing electrical wiring, it is a technology that can be easily deployed and adapted. From WiFi extension [13] over smart meters [32] to Electric Vehicle (EV) charging [22], including transmission of highly sensitive data, such as hospital communications [10], PLC has proven useful in many different domains, where high-speed data transmission is necessary. While multiple distinct variations of PLC exist, HomePlugAV became the de facto standard, backed by major electronics manufacturers. HomePlugAV PLC devices have become widely available for consumers at a low cost, while offering interoperability, plug-and-play functionality, and speeds of hundreds of megabits over distances of up to a hundred meters. As a result, PLC modems quickly became popular in domestic settings, where users desired to extend their network throughout the entire house, particularly to areas with poor coverage, without the necessity of installing new wires, and with greater robustness and throughput compared to WiFi. The website WiGLE [44], which offers an overview of WiFi networks, underscores the prevalence of PLC by filtering for devices with MAC addresses from recognized PLC manufacturers. For example, all devices from Devolo, a well-known manufacturer for PLC-to-WiFi adapters, share the same initial three bytes in their MAC addresses (i.e., `F4:06:8D`). Figure 1.1 depicts an overview of various interconnected devices in a typical household using PLC.

Over the years, several vulnerabilities have been reported in the implementation and use of HomePlugAV. For instance, research showed that HomePlugAV devices are vulnerable to Denial-of-Service (DoS) attacks [35, 42], as well as attacks against their pairing mechanisms [42]. With physical access to the victim's power lines, these vulnerabilities can be easily exploited, allowing an adversary to join the network and perform a range of network attacks. At this point, the adversary has access to the network as if they were directly connected to the network router or switch via an Ethernet cable [42]. All of these attacks can only be carried out with access to the power line, they are therefore referred to as wired attacks. While they can be very powerful, they require a

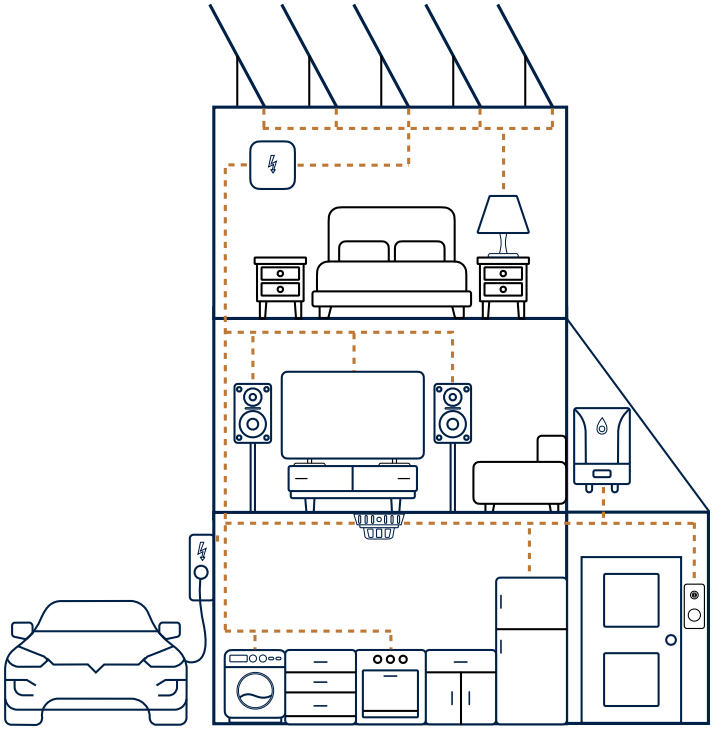


Figure 1.1: Illustration of the interconnection of various devices in a household via power-line communication.

direct physical connection to the victim's power lines, which greatly weakens the threat model of the attacker. However, the use of existing cabling, which is one of the key benefits of PLC, is also one of the key issues and increases the attack surface of PLC deployments. Compared to Ethernet cables where the standard demands shielding, power lines are not designed for the transmission of high-frequency signals, as used by PLC: their lack of proper shielding for these frequencies leads to the unintentional leakage of Electromagnetic (EM) waves outside of the medium [25], which makes PLC vulnerable to passive and active wireless attacks (i.e., without the need to be directly connected to the power lines). While effective, the latter require specialized and expensive equipment, such as software-defined radios, and digital signal processing expertise to implement, making them difficult for an attacker without extensive knowledge to execute. Additionally, their impact has less potential than wired attacks. For instance, in the Electric Vehicle charging domain, Baker [3] presents an attack with passive eavesdropping on the communication between the vehicle and its charger. Köhler [23] shows an active DoS, where communication preamble packets are sent repeatedly, leading to the abortion of charging. In both of the above, the full communication between devices is not shown and the attacks are limited.

In this paper, we show that wired attacks, which were believed to require direct physical access and connection to the power lines to be performed, can also be executed wirelessly. Compared to

previous wireless attacks, the advantage of our approach is the simplicity of the attacker setup. The setup for these wireless attacks consists of cheap, commercial off-the-shelf equipment, with no prior knowledge of signal processing required, making them easier to implement and achieve. With this in mind, this thesis evaluates the attack surface of HomePlug PLC deployments against a wireless attacker using off-the-shelf equipment and demonstrates the boundaries of such attacks.

In particular, we explore the previously established threat model against PLC and extend it by demonstrating the feasibility of executing attacks wirelessly, which were once thought to be limited to adversaries connected to the same power lines as the victim PLC devices. By employing readily-available hardware, we illustrate the potential for these wireless attacks, thereby challenging the conventional understanding of PLC security. Furthermore, we investigate the extent to which EM leakage can facilitate such wireless attacks on PLC systems. Through lab and real-world experiments, we assess the capabilities of both passive and active adversaries in leveraging EM leakage to compromise PLC networks. This analysis helps in quantifying the practical requirements and limitations for executing successful wireless attacks. Lastly, our findings debunk the common perception that physical access constraints significantly supports the security of PLC networks. We provide concrete evidence that a wireless adversary can eavesdrop on the communication up to 4 m away from the target building, and infiltrate a PLC network from a distance of up to 1.5 m using simple, commercially available equipment.

Chapter 2

Background

This section explains the various concepts and technologies discussed in the paper, with the goal of providing the reader with the necessary context to understand the rationale behind the attacks and the experimental setup.

2.1 Power-Line Communication

Power-Line Communication (PLC) designates a technology that uses the medium and low voltage electrical network to provide telecommunication services. It is most commonly used for high-frequency applications [4]. Some associations have a standardization role for PLC, the major actor in this process is *HomePlug Alliance*. Manufacturers for HomePlug Alliance groups cover both PLC technology and services, in order to develop HomePlug specifications, such as HomePlugAV. These specifications will be covered in more detail in Section 2.2. The necessity to create PLC arose with many new bandwidth-intense applications, where other wireless technologies - such as WiFi - have failed to meet the required quality of service, especially in the case of multiple applications or contending flows [43].

Once installed, PLC networks provide sufficient data rates for real-time transmission. Some of the possible applications of PLC include: voice and video (e.g., Telephony over PLC, Videoconferencing, Multimedia), building local networks (e.g., Internet connection sharing, Video Surveillance, WiFi Network), industrial applications (e.g., Connection of Programmable Controllers, Sensor networks), or even applications in public spaces (e.g., Authentication traffic for time clocks, Information feedback from beverage dispensers) [4]. Certain applications of PLC may involve transmitting highly sensitive and crucial data, such as hospital communications [10] or - in a different domain - communication between underwater vehicles and surface vessels [8]. In such scenarios, ensuring robust security measures for PLC technologies is essential.

In addition, wired Ethernet technologies require the installation of a new and costly infrastructure. PLC addresses this issue by being both easy to install and providing high data rates. As the name indicates, PLC uses existing power lines for data transmission. This enables devices to communicate through electrical wires and common power outlets, without the need to install any new wiring, making PLC cheap and easy to deploy. On the flip side, using a pre-existing medium poses new challenges. Traditionally, when looking at power exchanges, there is no need to shield against EM radiations. However, signals with higher frequencies, as used in PLC technologies, tend to radiate more effectively. The lack of shielding of power cables makes the medium exploited for PLC not perfectly adapted to the latter [29], making PLC deployments prone to EM radiations. Indeed, even if the emitted disturbing field of PLC devices does not affect the activity of the PLC network itself [20, 34], the technology is sensitive to EM interference and interception [25]. Broadband PLC adapters, when transmitting across a wide range of frequencies, will almost always generate detectable radiation within the spectrum. This occurs as a result of certain sections of the nearby electrical wiring unintentionally acting as a convenient antenna. The potential issues arising from these emissions are broadly recognized, prompting academic research and regulatory measures. While these efforts aim to minimize unintended emissions [24, 33], no leakage can be fully removed and PLC technologies are still vulnerable to EM interference and interception.

2.2 HomePlugAV

The standard for broadband PLC technologies is defined by the *IEEE 1901* project [21]. The dominant technologies ratified by this standard are the HomePlug families and, more specifically, *HomePlugAV* [26], as most its functionalities are used in later standards (e.g., *HomePlug Green PHY* [19]). HomePlugAV has a signal bandwidth of 28 MHz and operates on existing power lines in a frequency range of 2 MHz to 30 MHz. To achieve high throughput, HomePlug uses Orthogonal Frequency Division Multiplexing (OFDM) [28]. Defined as a multicarrier modulation technique, this method involves dividing a high data rate modulating stream into slowly modulated narrowband close-spaced subcarriers. This modulation technique was chosen as it is robust against frequency selective fading or impulsive noise, and resilient to narrow band interference. It distributes a total of 1,155 subcarriers over the frequency range [18].

Network Architecture: The standard employs a virtual network mechanism, known as AV Logical Network (AVLN). It encompasses HomePlug stations (i.e., devices) interconnected via the AC powerline. While physical-layer connections may extend across dwellings, HomePlugAV logically separates stations by using a privacy mechanism based on a 128-bit AES encryption scheme in CBC mode, tied to a unique Network Encryption Key (NEK), which is responsible for encrypting data payloads and undergoes periodic changes. An AVLN constitutes a set of stations sharing a common Network Identifier (NID), which identifies the network, and Network Membership Key (NMK) [26], which a new station needs to join the AVLN. The latter can be obtained by a new station through different

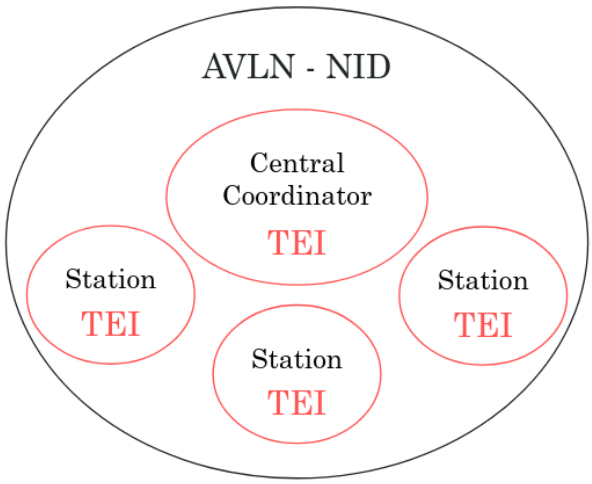


Figure 2.1: HomePlugAV: AV Logical Network (AVLN), identified by its NID, with a Central Coordinator and three Stations, each identified by their TEI. [4]

pairing mechanisms provided in HomePlugAV (e.g., Push button, Manually configured through the user interface). New station authentication relies on the NMK, allowing successful authentication and association within the AVLN, where each station is assigned a unique Terminal Equipment Identifier (TEI) during the association process. All HomePlugAV transmissions incorporate source and destination TEIs for addressing purposes.
Each AVLN designates a specific device as the Central Coordinator. The Central Coordinator performs the management role within each AVLN, overseeing network functions, such as authentication, association of new stations, AC line cycle synchronization, admission control, and scheduling CSMA sessions and allocations. Periodically, the Central Coordinator emits synchronization beacons within the AVLN to align with the AC line cycle and disseminate management messages. Figure 2.1 shows a schematic representation of an example of a HomePlugAV Logical Network and different devices it contains.

Data Transmission: In order to perform data transmission, PLC stations prepare Data Frames: data blocks with a header and an area indicating the end of the frame. Since the power line medium is shared, finding a way to manage multiple frames from different devices is important. Frames sent over the physical layer have a structure where a second frame is enclosed within the first. Figure 2.2 depicts how data is transmitted in the PLC architecture using the MAC layer (i.e., Data Link) and physical layer (i.e., Physical Link). The initial layer deals with accessing the power line medium, and the frame for this protocol is called the MAC Protocol Data Unit frame. All data from layers above the MAC layer is wrapped within the MAC frame. This MAC frame is then enclosed within another frame at the physical layer to transmit it over the physical or electrical interface. This enclosed frame is known as the Physical Protocol Data Unit.

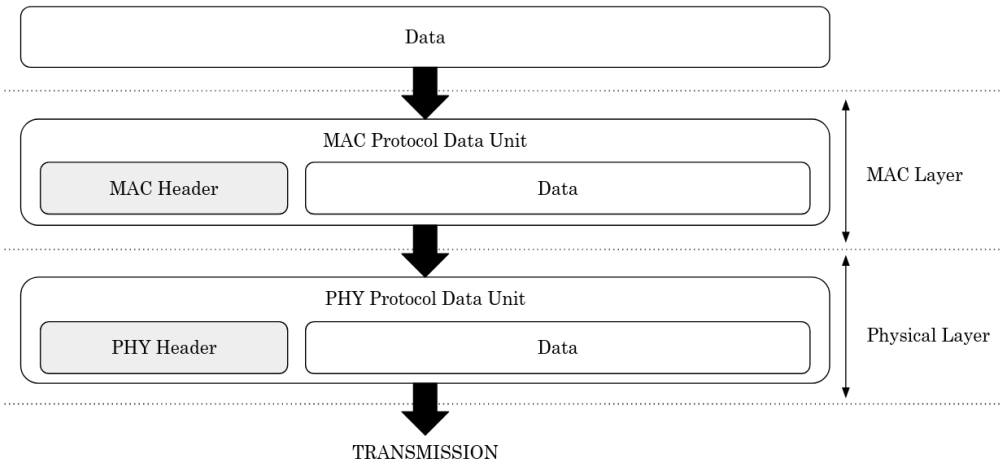


Figure 2.2: HomePlugAV: Data Transmission [4]

HomePlugAV supports adaptive bit loading. It enables each subcarrier to be modulated in order to achieve the highest possible data rate based on the received signal strength. For instance, a subcarrier with low received signal strength might support Binary Phase Shift Keying, which provides 2-bits per subcarrier per symbol. At the other extreme, a subcarrier with very high received signal strength could support 1024 QAM, which provides 10-bits per subcarrier per symbol. The implementation of adaptive bit loading within the OFDM signal facilitates maximizing data transmission on each subcarrier according to specific line conditions. However, this technique necessitates prior knowledge of the signal strength for each subcarrier at the transmitter before packet transmission. Consequently, HomePlugAV devices within the network periodically exchange sounding packets to continually update and retain channel condition information in the form of Tone Maps, which describe the signal level for each subcarrier within the OFDM signal. Moreover, the standard enforces several higher-level management systems. These systems address quality-of-service provision, coexistence with other virtual networks, and network extension via relays. Communication protocols are established for managing the virtual network, exchanging Tone Maps between device pairs, and ensuring inter-network cohabitation, maintaining a consistent minimum traffic level when a device is connected and powered.

The fundamental channel access scheme utilized by the HomePlugAV MAC is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). As it operates on a collision-avoidant principle, prior to transmitting a data packet, each device actively monitors the network it is part of. If one device is already transmitting, other devices defer their transmission until the line becomes idle. When the medium is clear, network stations prioritize and resolve pending traffic, ensuring that the highest-priority traffic gains access to the medium for data transmission before individual stations can initiate their transmissions.

2.3 Network Detection and Traffic Sniffing

2.3.1 Sniffer Mode

Most PLC devices have a *sniffing* feature that, once activated, allows them to detect the presence of other PLC devices located on the same electrical network, if the signal is strong enough, without necessarily being part of the same AVLN. It can be activated by sending a `SNIFFER.REQ` message to the PLC device through a direct physical connection to its Ethernet interface, which requests the activation of the sniffer mode on the device. Once the sniffer mode is correctly enabled, the device responds with `SNIFFER.CNF`, which confirms that the request has been processed. The HomePlugPWN tool suite [15] provides a script to trigger the sniffer mode. It can also be enabled using the Open-PLC-Utils [36] suite. Once the sniffer mode is activated, the device wraps all received MAC frames within Ethernet frames, and makes them accessible through its Ethernet interface for capture, using tools like `tcpdump` [40]. This can all be done live and does not induce any processing overhead because all the demodulation is done by the PLC modem itself. It is important to note that, while these frames can be captured, only the header information is fully demodulated, with the payload content remaining partly undisclosed.

2.3.2 Wireless Traffic Reception

As mentioned in Section 2.1, PLC technologies are prone to EM radiations, which can be wirelessly captured by devices that are not physically connected to the network. This implies that signals transmitted on the power line by the PLC devices that are connected to it can be captured from a distance and interpreted accurately, with the correct receiving chain. Exploiting this unintended feature to our benefit, we can enable the sniffer mode on a PLC device and use it to receive and demodulate HomePlug packets wirelessly. Thus, this features allows us to identify a network of PLC devices, gain information about its topology and individual devices, and sniff the traffic between these devices, without necessarily being physically connected to the electrical network, thanks to the radiations coming out of the power lines. In addition, in the real world, to prevent the leakage of PLC signals via the power lines to adjacent apartments and houses, attenuators and filters can be used. However, these are ineffective against a wireless attacker, given that the signal is radiated by the wires between the PLC modem and the filter.

Beacons: The packets captured and demodulated by the sniffing PLC device can be divided into different categories depending on the type of information they carry. Multiple packet categories exist and can give away information about the network and its communication. For instance, Beacons are commonly used by the Central Coordinator. They play an important role in network management, controlling channel access and topology discovery for stations, either inside or outside of an AVLN. All Beacons share the same format, but can have different content based on the Beacon Type [26].

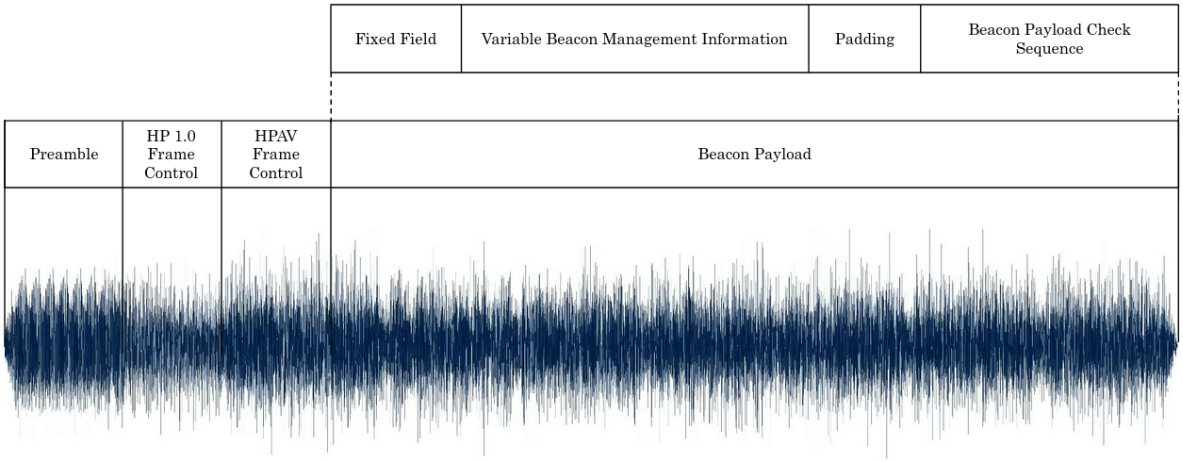


Figure 2.3: Beacon Format and Waveform [26]

Figure 2.3 shows the Beacon format with the shape of its waveform in the time domain associated to its different components. This includes an HP1.0 Frame Control and a 128-bit Beacon Frame Control followed by 136-octet Beacon payload. Beacon payload includes some fixed fields (i.e., fields present in all Beacons) followed by variable Beacon Management Information. The latter includes the Network Identifier of the AVLN of the transmitting device, and one or more Beacon Entries. Depending on the need, different sets of Beacon Entries will be included in the Beacon.

Beacon Entry: As mentioned above, a Beacon Entry is a field contained in Beacons, which is used to carry information. Various types of Beacon Entries exist, each with a different purpose, with specific interpretations depending on the Beacon Entry Header. Some examples of Beacon Entry types include: MAC Address Beacon Entry, Central Coordinator Handover Beacon Entry, Encryption Key Change Beacon Entry, etc. The Beacons received by the sniffer are mainly Discover Beacons [18] because they are the ones which are periodically sent by PLC devices in a network to understand the network topology, especially if changes occurred. In Discover Beacons (i.e., Beacons transmitted by all devices in the network for network-topology discovery), it is mandatory to feature a MAC Address Beacon Entry [18], but it is optional in other types of Beacons. MAC Address Beacon Entries specify the MAC address of the station that transmits the Beacon. Extracting this information allows us to uniquely identify a device and, combined with the NID, determine which network it is part of.

Network Identifier (NID): Each AVLN has a 54-bit Network Identifier (NID) that uniquely identifies the network. The NID is generated by combining the Security Level (2 bits) with the NID Offset (52 bits) as shown in figure 2.4. Essentially, the default NID Offset is generated by hashing the NMK using SHA-256 as the underlying hash algorithm. The Security Level is set to 0b00 when push-button-based authentication is used. In all other cases, Security Level is set to 0b1. By retrieving this field from the Discovery Beacon received by the sniffer, we determine which network the detected device is part of. From the construction protocol of the NID, we can also obtain a hint for

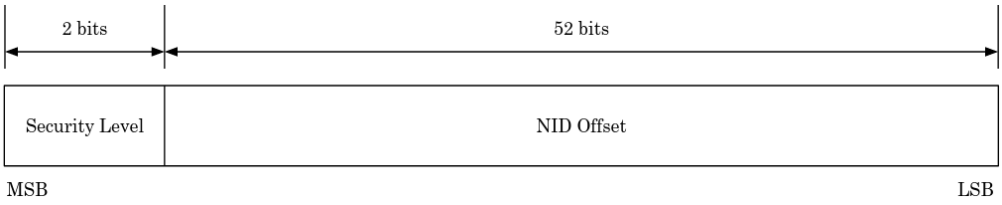


Figure 2.4: Network Identifier (NID) Construction [26]

the underlying NMK as "a hash-value serves as a compact representative image of an input string, and can be used as if it were uniquely identifiable with that string" [31]: the hash of the same NMK will always be the same. Thus, if we know the NID associated to a default NMK value, we can recover the NMK from this NID when encountered.

2.4 Related Work

In the past years, research has shown that PLC technologies can be vulnerable to various attacks. In particular, the security of HomePlug devices was investigated and several attacks were developed. These attacks, and in particular wired attacks, serve as a motivation for this thesis.

Scholz and Wressnegger [38] analyzed the security of Devolo [1] - one of leading manufacturers offering products with PLC technologies - HomePlug Devices. They showed that there was a worrying number of devices still using default configurations, including the default NMK: "HomePlugAV", which we demonstrate is still the case nowadays. In fact, we bought the top adapters from the four major domestic PLC manufacturers (i.e., devolo, tp-link, Mercusys, and Netgear), from Amazon, and prove that they are all shipped with default NMK.

Wired attacks have been performed on PLC technologies i.e., attacks where the attacker is directly connected to the power line. A selection of wired attacks can be found in Table 2.1, including the list of the requirements needed to perform each attack, as well as the goals that could be achieved by an attacker. All listed attacks require the attacker to have a PLC device and the latter has to be connected to the same power line as the target PLC network. This physical connection is necessary to perform various intrusive actions, ranging from passive eavesdropping to active network interference. Passive attacks involve observing communications to gather confidential information about the network, its devices and users. In contrast, active attacks seek to disrupt network operations or gain access to the targeted AVLN.

The Minimum-Effort and Covert attacks [2] illustrate how attackers can perform bulk data exfiltration, real-time traffic monitoring or prepare a platform for further attacks. The main requirement for these attacks is to have temporary physical access to the premises in order to set up a malicious PLC device on the same power line as the target network. The key difference between the two attacks

is in how the malicious device is concealed. In the Covert attack, the attacker can discreetly connect their device to the existing power line infrastructure, which is usually out of sight within wall cavities. In the Minimum-Effort attack, the adversary plugs in his malicious PLC device into one of the wall sockets of the victim's building. The device will be visible, but it is the setup that requires the least effort for the adversary.

The DoS attack presented by Puppe et al. [35], leveraging limited buffer size for received packets and packet decryption times, showcases how attackers can saturate network resources, leading to disruption of the network and blocking access to its resources, targeting the whole network and not only devices within range. This attack does not need the attacker to have access to the target AVLN, it can be performed with any device. Another DoS attack is presented by Uwaezuoke et al. [42] where the additional requirement to the previous attack is to have access to an open port from one of the PLC devices as they often are Universal Plug-and-Play-enabled network devices. Using this open port, the adversary can flood the network layer with multiple MAC requests and DHCP discovery requests, resulting in a Denial-of-Service.

In the context of Electric Vehicle charging, the Vehicle-to-Grid (V2G) Injector [16] shows an attack on V2G systems that communicate via power lines support. The authors develop a new tool to interface with these systems, to analyze them, and to inject data through power plugs if an installation shares the same network as the Electric Vehicle charging stations, leading to the ability to analyze exchanged packets and craft them to attack different controllers and units. They use a specification vulnerability in the communication medium to exploit and intrude the V2G network.

In Research Project: HomePlug Security [35], the authors present a dictionary attack on the Network Encryption Key (NEK). Once again, the adversary has to own a malicious device which is connected to the target power line. They join the target AVLN by repeatedly changing the NEK of the malicious device and attempting to join the network, until the procedure succeeds. By carefully crafting the dictionary used, the authors were able to perform the attack with success in less than 20 min 30 sec.

In 2014, Tasker [39] presented an attack on the Device Access Key (DAK). The DAK can be used to join its associated AVLN and the author shows that the DAK of a device can be derived from its MAC address. The MAC address of devices can easily be obtained by sniffing the traffic with a rogue PLC device, connected to the same power line, and intercepting HomePlug packets. In 2016, the DAK derivation was changed from a deterministic algorithm based on the device's AC address to an algorithm based on `/dev/urandom`, which can be considered as more secure. Old devices which received an update, or newly manufactured devices, benefit from this fix. This implies that there might still be old devices which were not updated that are still affected by this vulnerability. The K.O.DAK attack [14] targets the DAK as well. The authors observe a pattern in different DAKs and use it to develop a dictionary attack. Once the DAK of the Central Coordinator is obtained, they change the NMK of the target AVLN to integrate it. This grants the adversary internet access, provided that the PLC devices within the network were configured to facilitate such connectivity.

In Powerless Security [17], the authors present several attacks on the pairing methods of PLC devices (i.e., the protocols used to join an AVLN). The first attack is on the Network Membership Key (NMK). The attacker initiates this process by capturing at least one MAC frame that contains a set-key request (i.e., a request encrypted under the NMK). This request is intended for a device joining the network. The attacker employs a dictionary-based approach, cycling through potential NMKs and applying each to decrypt the captured MAC frame. Successful decryption is verified by matching against 16 bits of predetermined plaintext. In the same paper, an attack on the Pairing-Button method is presented: the attacker keeps their malicious device in pairing mode, until the user triggers the pairing process on their end, which allows the malicious device to join the network at the same time as a legitimate device.

The Evil Twin with Captive Portal attack [42] aims at eavesdropping and capturing login credentials on the wireless communication channel, initiating a new AVLN or joining an existing AVLN by forcing the Push-Button virtually. The attacker mimics a legitimate wireless access point to intercept login credentials. This active strategy involves creating a decoy access point, through PLC, with the same name as the real one, then forcing devices to connect to it by de-authenticating the legitimate access point. Once users connect to the fake access point, their login information, including usernames and passwords for the AVLN adapters and the wireless network, is captured.

The Bruteforce Attack of WPA/WPA2 Password [42] is an attack against PLC devices serving as wireless access points for the WiFi network supported by the underlying AVLN. The attacker needs to have access to the wireless traffic data, which can be the case if they succeeded in joining the legitimate AVLN with their malicious device. Then, with enough processing power, they can bruteforce the WPA/WPA2 password of the WiFi network and penetrate it. The authors were able to show that with the combined power of several GPUs, the password could be obtained in 120 min.

Finally, a Machine-In-The-Middle (MITM) attack [42] is presented, which aims at intercepting link-layer data frames of the AVLN. In this attack, we assume that the attacker's PLC device has gained access to the target AVLN, possibly using the techniques mentioned earlier. The objective of the attack is to associate the malicious device's MAC address with the IP address of the Central Coordinator of the target AVLN. With this procedure, the adversary's device can intercept any unencrypted transmitted data frames (e.g., IP camera controls, Home-automated gadgets input commands).

For all of the wired attacks that were mentioned, each one of them requires the adversary to possess a PLC device physically connected to the power line of the target AVLN. Without this requirement, none of these attacks were deemed possible. We extend previous research on PLC security by demonstrating, through laboratory and real-world evaluation, that the necessary conditions for both passive and active attacks are achievable wirelessly, without physical access to the target power line, with affordable off-the-shelf equipment and no prior knowledge in signal processing. We demonstrate how EM emissions from PLC networks can be exploited to wirelessly capture and inject communication packets, bypassing the need for a physical, wired connection to the power

line. In addition to making claims about a stronger adversary (i.e., who can be at a distance from the victim), it also makes all previously wired attacks more scalable, not restricted to a single target, especially if several houses with PLC deployments are close to each other.

Some wireless attacks have also been explored in recent research, orthogonally to previous wired attacks approaches. They show that some wireless attacks can be performed on PLC technologies, i.e., attacks where the attacker does not have a device connected to the power line of the targeted network. In the context of EV charging, Baker [3] presents passive eavesdropping of EM radiations from EV charging communication. The unintentional wireless channel is sufficient to recover messages in most cases, reaching a rate of 91.8 % of messages validating their checksum when intercepted from an adjacent parking bay. By observing the recovered traffic, the authors could find privacy and security issues in the existing charging infrastructure e.g., absence of TLS enforcement in public locations and leakage of private information. Brokenwire [23] is an active attack against Combined Charging Systems, which are widely used in Direct Current rapid charging technologies for EVs. By exploiting a vulnerability in the communication protocol, they perform a DoS attack which interrupts the control communication between the vehicle and the charger, leading to the abortion of charging. One can execute this attack in person or even remotely, if the device is deployed at the target site. The attack requires only temporary physical proximity and can be conducted wirelessly from a distance.

Both of the wireless attacks presented are impactful, yet their execution necessitates considerable investment in specialized, costly equipment such as software-defined radios, alongside a requisite proficiency in signal processing. This requirement restricts the feasibility of these attacks, and makes it difficult for any potential attacker to execute. On the other hand, the approach detailed in our study leverages affordable, commercially available hardware, eliminating the need for advanced signal processing expertise, while still showing significant impact.

Table 2.1: Selected Wired Attacks on HomePlugAV and their Characteristics

Attack Name	**Category**	**Goals of the Attacker**	**Requirements for the Attack**
Minimum Effort & Covert Attacks [2]	Passive	Bulk data exfiltration, Real-time traffic monitoring, Platform for further attacks	Temporary access to premises to install a (hidden) PLC adapter on the power line of the target network
Denial-of-Service (DoS) Attack [35]	Active	Disrupting the network and blocking access to its resources	PLC device connected to the same power lines as the target network
DoS: DHCP and MAC Request Flooding Attack [42]	Active	Disrupting the network and blocking access to its resources	PLC device connected to the same power lines as the target network, Access to as open port
V2G Injector: EV Charging [16]	Active	Intruding a V2G network	Has a PLC device impersonating the charging station which is connected to the same power lines as the target network
NEK Dictionary Attack [35]	Active	Join the target AVLN	PLC device connected to the same power lines as the target network
Attacks on the Device Access Key (DAK) [14, 39]	Active	Join the target AVLN, Penetrate neighbour's LAN	PLC device connected to the same power lines as the target network
Offline Dictionary Attack on NMK [17]	Active	Join the target AVLN	PLC device connected to the same power lines as the target network
Breaking Unicast Key Encryption Protocol: Pairing Button [17]	Active	Join the target AVLN	PLC device connected to the same power lines as the target network
Evil Twin with Captive Portal Attack [42]	Active	Eavesdrop and capture login credentials, Initiate a new AVLN, Join existing AVLN by forcing push button virtually	PLC device connected to the same power lines as the target network
Bruteforce Attack of WPA/WPA2 Password [42]	Active	Penetrate wireless networks established through PLCs	PLC device connected to the same power lines as the target network, Access to wireless taffic data
Machine-In-The-Middle (MITM) Attack [42]	Active	Intercepting the link-layer data frames	PLC device connected to the same power line as the target AVLN, Gained access to the target AVLN

Chapter 3

Threat Model

Our considered adversary could have multiple goals. These goals are already defined and explored in the wired attacks that are described in Section 2.4, which serve as motivation for our work. Table 2.1 shows a selection of wired attacks on HomePlugAV where the goals of the attacker are presented for each of them. As they are already described extensively in their corresponding publications, we give a brief overview:

Obtain Knowledge: An Honest-but-Curious attacker aims to learn about the victim's network, revealing critical information about the victim. This poses a significant privacy threat, as some of the crucial data that could be inferred includes: time of day when the network is mostly used (i.e., indicating the victim's presence), network's topology and devices, communication patterns, etc. If the attacker turns malicious, they could easily track the victim's activities through traffic monitoring, without needing direct network access (i.e., the adversary does not need to be part of the target AVLN). This could be the initial step in preparing for a subsequent physical attack.

Gain Network Access: An attacker who gained access to the victim's network (i.e., AVLN) could perform most network attacks that can be implemented when a malicious adversary has infiltrated a network, similarly to WiFi. PLC vulnerabilities open the door to new ways of infiltrating a network.

Denial-of-Service: An attacker's aim could be to perform a DoS of the victim's PLC network to prevent them from accessing any of its resources. They could establish the attack on a targeted victim to block any type of communication for a certain period of time.

In each of the cases described, the attacker is targeting a specific network. In a domestic setting, the attacks can target any person connected to the home network. In an industrial setting, the attacker could target any company that is using the network. Overall, all of the categories mentioned above could allow an adversary to cause financial loss, perform blackmail, gather information about

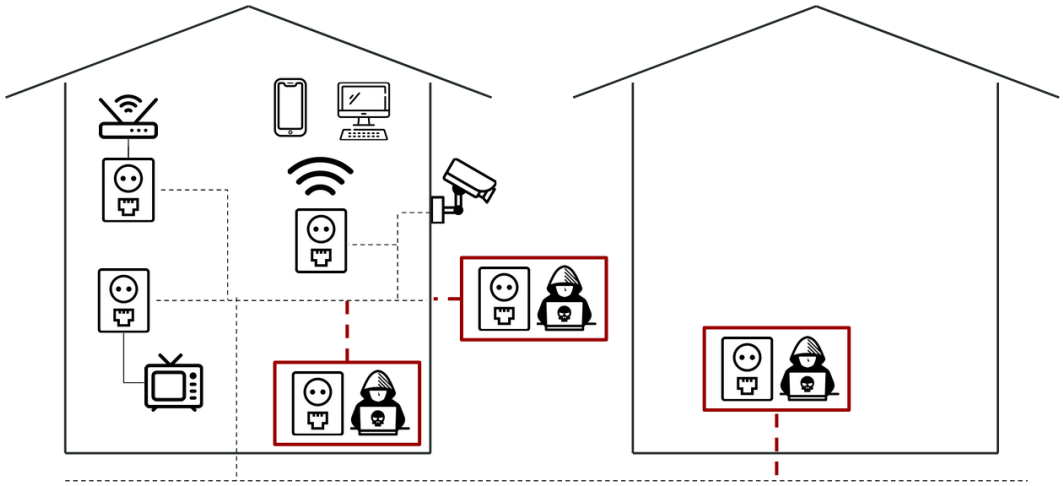


Figure 3.1: Previous Threat Model for the Wired Attacks

the target, or simply disrupt the normal behavior of the network.

As Figure 3.1 shows, the previous threat model for wired attacks entails an adversary who has access to the power line to which the victim network is connected. It assumes that the adversary has a PLC device that they can connect to the victim's power lines - either through a socket or by directly accessing the cabling. However, our threat model makes stronger claims by considering an adversary who does not have direct physical access to the victim's power line (e.g., No access to any of the power sockets or wiring on the victim's power line), but can still perform the attacks of the previous adversary. The attacker can choose not to physically connect to the power line and perform their attack from a distance while achieving the same results.

Likewise, the threat model described is stronger than the one used in previous wireless attacks [3, 23] because only cheap off-the-shelf equipment is used, which can be purchased for around 20$, and no specific signal processing knowledge is necessary to understand and perform the attacks. Our adversary could be any curious or ill-intended person as none of the attacks are complex. To increase attack distance and efficiency, they might purchase a directional antenna and suitable equipment for amplification.

Chapter 4

Lab Evaluation

In this section, we present the results of our experiments conducted within a controlled laboratory environment, aimed at evaluating the key parameters involved in performing the attacks. This isolated laboratory context, where parameters were controlled and explicitly defined, provided us with insights into the system's behavior and what influences it. In Section 5, we further investigate the performance and limitations of performing wireless attacks in a real-world environment. The source code for lab and real-world evaluations can be found in Section A.

4.1 Experimental Setup

4.1.1 Device Components

Figure 4.1 shows a schematic of the equipment for the experiments, which we describe below:
Raspberry Pi 4: Acting as the main machine of the device, the Raspberry Pi takes care of all the processing of the packets received by the sniffer. It filters out packets that are not related to the Power-Line Communication i.e., not from the HomePlugAV protocol, extracts the relevant information from each packet (e.g., MAC address and Network Identifier) and gathers information about the experiments along their execution (i.e., HomePlug Packet Rate, Ping Success Rate). It also takes care of all the coordination between different modules that constitute our final device (e.g., activating the sniffer mode of the PLC modem).

HomePlug PLC Modem: With the sniffer mode enabled, this PLC modem serves as a receiver for any packet that could be intercepted coming from external PLC devices, whether part of the an AVLN or not. Then, it makes the sniffed packet accessible to its Ethernet interface, ready for capture with `tcpdump` [40], in this case. In order to improve the reception power of the device, we linked a dedicated antenna to the modem.

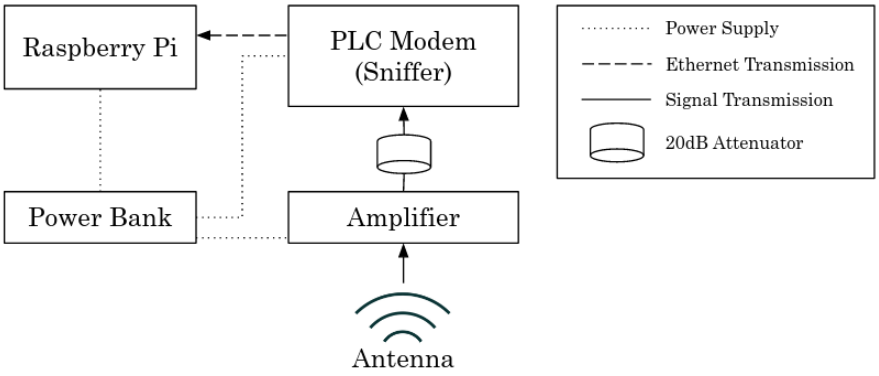


Figure 4.1: Overview of the different components we used to conduct our evaluation and how they were interconnected.

Antenna: The antenna is one of the key components of the detecting device. It improves the attack reach of our device and greatly impacts its detection rate. In this study, we used two different antennas, each fulfilling a different use case.

Whip Antenna of 40 cm: The Whip Antenna consists of a straight rod and its bottom end is connected to the receiver (or transmitter). This antenna is a monopole antenna, in reference to the presence of only one physical side [6]. The one used in our experiments is 40 cm long, which makes it very convenient to carry as, in movement, it can be held by one person only. It could even be carried in a backpack while walking, where no one would notice the complete device. As a side note, holding the antenna by hand makes the user an extension of the antenna as well, which slightly improves the detection reach of the device.

Dipole Antenna of 10 m: The Dipole Antenna consists of two conductors of equal length, oriented end-to-end with the receiver connected between them. It can be made out of metal wires where the length of both wires is the same and each strand of wire is extended to opposite sides. The antenna used in our setup is a full-wave dipole, where each wire's length is half the wavelength of the signal we wish to receive. As the frequency range of HomePlugAV is between 2 MHz to 30 MHz, the minimum length for a full-wave dipole antenna for this frequency range [30] is $\lambda = \frac{v}{f} \simeq 10\,\text{m}$ [5]. In contrast with the previous antenna, the full-wave dipole antenna cannot be carried by a single person when in movement. However, once the location of the attack is determined, it can easily be spread out and does not necessitate multiple people to manipulate it.

Amplifier: In order to improve the reception of our setup, we added an amplifier which improved receiving rate as it amplifies the HomePlugAV signals received by the antenna. We also explored the use of a Low-Noise-Amplifier (LNA) to improve the quality of the received signal, but a lot of noise was induced and worsened the receiving rate, which is why we decided not to use it in the final device. As Figure 4.1 shows, a 20 dB attenuator was connected between the amplifier output

Figure 4.2: Picture of a simple setup for the adversary's device consisting of a commercially-available PLC adapter acting as the sniffer, a Raspberry Pi, an extension cable of variable length, and a power bank to power the setup.

and the PLC Modem. The attenuator was necessary to protect the amplifier from the TX channel of the PLC modem (i.e., Sniffer). Similar to any other PLC device, the sniffer periodically sends packets (e.g., Beacons to learn about the network topology). Without the attenuator, these signals would reach the output stage of the amplifier and potentially cause permanent damage. For experiments that required bidirectional communication, attenuator and amplifier were removed. Transmission and reception simultaneously with amplification could be achieved with a different setup, but it would need additional equipment and make the final device less portable.

All the equipment mentioned is affordable and can be assembled without deep technical skills. However, if one wants to use an even more minimalist setup with cheap and off-the-shelf equipment, they can use an extension cable as antenna (i.e., the antenna length is defined by the length of uncoiled wire), with a PLC device plugged in (e.g., a basic WiFi extender) connected through Ethernet to a machine (e.g., a Raspberry Pi), and a power bank to power the complete setup. Figure 4.2 shows a picture of this type of setup with its components and their connection. With the correct length of uncoiled wire from the extension cable, a full-wave antenna can be created. Testing this setup in the scenarios presented proved to be as efficient as our slightly more complex setup.

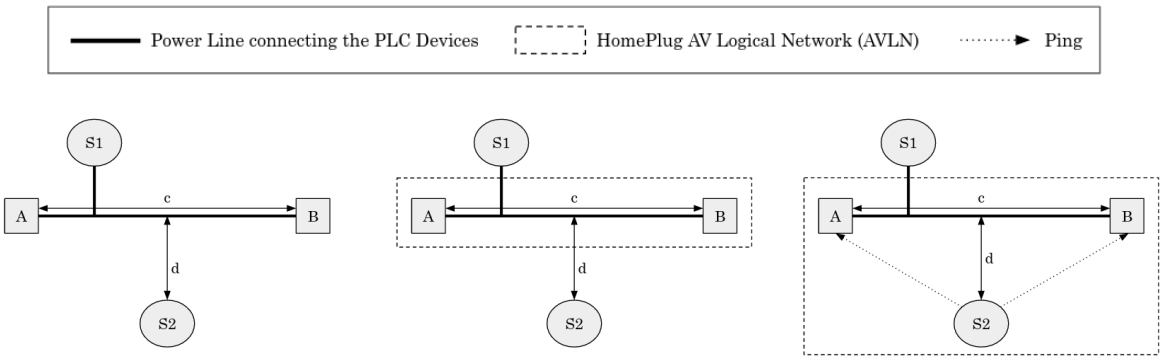
4.1.2 System Setup

Two main scenarios were used to perform the experiments. In both scenarios, the same devices were used, presented in Table 4.1. The components of the system and setup common to all scenarios are depicted in Figure 4.3a. It illustrates the three parameters that were varied throughout the experiments, which are described below.

Cable Length c**:** The cable is connecting the PLC devices A, B and $S1$ to each other. It corresponds to the power line on which communication occurs. Essentially, a cable can act as an antenna due to its construction with conductive material, such as electrical wires, which undoubtedly affects the reception and transmission capabilities of our device. This is why we found it valuable to experiment with varying its length.

Device	Manufacturer	Role
S1	Devolo	Sniffer on the Power Line [12]
S2	Devolo	Adversary's PLC Modem [11]
A	TP-Link	PLC Adapter Connected to Machine A [41]
B	TP-Link	PLC Adapter Connected to Machine B [41]

Table 4.1: PLC Devices and their Roles.



(a) Basic Setup. (b) Scenario 1: Sniffing. (c) Scenario 2: Injecting Data.

Figure 4.3: Base setup and experimental scenarios depicting the varying parameters of the system: length c of the cable connecting the PLC devices A, B, and the power line sniffer $S1$, and distance d between the victim system and the attacker $S2$.

Distance d between the Adversary's Device and the System: This is the most influential parameter of this study. Varying the distance between the device and the system allows the assessment of the efficiency of our device: the longer the distance at which we can still receive or transmit packets, the more powerful the adversary is. For each distance, we measure the received or successfully transmitted packet rate from our wireless setup.

The Antenna of the Adversary's Device: We used two types of antenna in the experiments (i.e., The Whip antenna and the Dipole antenna), which were described in Section 4.1.1. We explored each scenario with both antennas to see how it impacted potential attacks and their efficiency.

Our initial experiment focused on verifying that the control sniffer ($S1$) and the wireless sniffer ($S2$) would capture HomePlug packets at the same rate when both were connected to the same power line. This experiment aimed to confirm that, under identical conditions, both sniffers would record the same rate of HomePlug packet transmissions. Once this claim was established, we could use $S1$ as a control sniffer on the power line, which recorded the maximum packet reception rate,

and $S2$, as part of the adversary's device, which measured wireless packet reception rates at different distances from the system setup. For this purpose, $S1$ was physically connected to the power line shared by devices A and B, establishing a baseline for the number of packets transmitted within the network over the power line, while simultaneously using $S2$ to sniff for those packets. This is how we could evaluate how well the wireless sniffer $S2$ was performing in terms of packet reception.
Before discussing the experimental scenarios, it is important to mention that $S1$ is part of the system setup, as can be seen on Figure 4.3a. It is not part of the AVLN that is established between the PLC devices A and B in Scenario 1 (Figure 4.3b), and not part of the AVLN established between PLC devices A, B and $S2$ in Scenario 2 (Figure 4.3c). Thus, $S1$ serves as a control element for our evaluation, especially for Scenario 1, as it measures the real packet rate going through the system's power line, as opposed to the wireless sniffer $S2$ which measures the packet rate at various distances from the power line.

4.2 Scenario 1: Passive Adversary, Only Receiving

4.2.1 Method

In this scenario, we explored a passive adversary who tries to sniff HomePlugAV packets exchanged between the two PLC devices, A and B, physically connected to the same power lines and part of the same network (i.e., AVLN). This experiment evaluates the maximum distance at which the adversary could position themselves to receive traffic from the target network for a given setup. Each PLC device in the network was connected through Ethernet to a PC, and both PCs constantly communicated with each other. Machine A pinged Machine B with 64 B/sec of Internet Control Message Protocol (ICMP) data bytes [27]. We measured the amount of HomePlugAV packets that were received by $S1$ and $S2$ over 5 runs of 60 seconds for each distance d, for each cable length c, until no HomePlug traffic was observed by the sniffer $S2$. It is important to note that, in this experiment, we assumed that the NMK of the AVLN was unknown to the adversary. In other words, the attacker has not gained access to the network to perform their attack. As a result, both of the sniffers were not part of the AVLN. While in this setting, the attacker cannot actively interfere with the PLC network, the information and insights gained from the observations are still valuable and can be the starting point of more sophisticated attacks.
This scenario represents an adversary who either wants to detect the presence of a network or, if they are already aware of the existence of this network, is willing to obtain knowledge about the victim's network, for example, to brute-force the DAK [14]. This could be the first stage to a more complex attack, where the adversary wants to eventually gain access to the victim's network by evaluating some of its characteristics. Figure 4.3b gives a visual representation of this scenario.

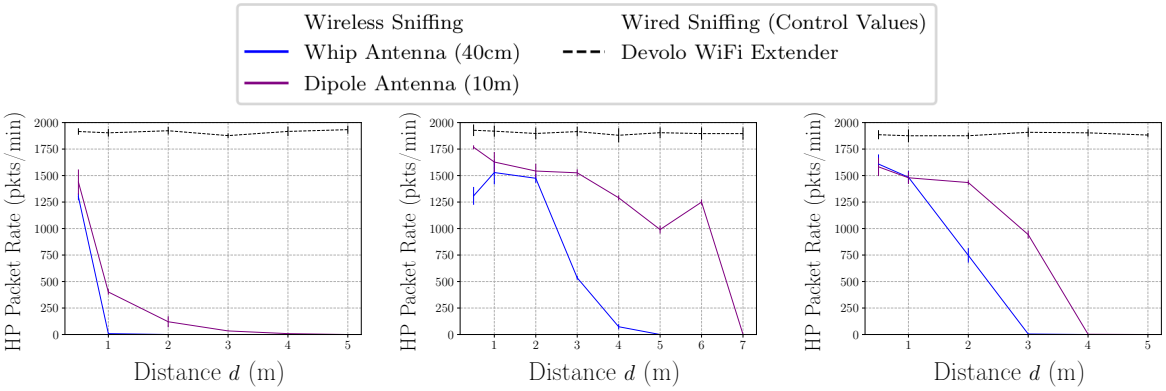
4.2.2 Metrics

To quantitatively assess each scenario, specific metrics were used to measure the effectiveness and reach of the adversary. These metrics provide a clear measurement of the adversary's impact but also give insights on the influence of each parameter on the experiments. In Scenario 1, the adversary has a passive role focused on intercepting communications. Thus, the primary metric of interest is the received HomePlug packet rate. This rate is expressed in packets per minute (packets/min) and serves as a direct indicator of the adversary's ability to successfully receive and demodulate HomePlug packets transmitted between devices A and B. We can then compare it to the HomePlug packet rate measured by the sniffer on the power line, acting as control values, to evaluate how well our device is performing. It should be mentioned that all sniffed packets are following one of the HomePlug protocols. Thus, it is not restricted to the HomePlugAV protocol, but also includes all of its derivatives (e.g.: HomePlug GreenPHY) that can be used by other devices than domestic PLCs.

4.2.3 Results

The effectiveness of our device in this scenario can be seen in the graphs of Figure 4.4. The graphs show the HomePlug packet rate for each distance between the system and our device, for each antenna, with a different graph for each cable length. It is interesting to note that an adversary could be up to 6 m away and still be able to sniff some packets, in the context of a power line of 3 m, using the dipole antenna. Additionally, we observed that the whip antenna can also be used to sniff packets from a distance: it is very efficient when close to the power line with at least half of the total number of packets intercepted when 2 m away from the power lines for a cable of at least 3 m. However, the whip antenna suffers from drastic efficiency drops when moving away from the system. Interestingly, Figure 4.4a properly depicts the Inverse Square Law [37] which states that the radiation intensity is inversely proportional to the square of the distance between the device and the source point.

In addition, our analysis highlights a critical security flaw in domestic PLCs implementing Plug-and-Play. This convenient setup allows devices to instantly establish an AVLN and join it upon being plugged into the power line, without requiring any configuration from the user. However, we discovered that devices from various manufacturers (i.e., devolo, tp-link, Mercusys, and Netgear) all share a common default NMK: "HomePlugAV". This universal NMK facilitates easy network establishment for the user, but severely undermines security. The HomePlugAV White Paper [19] acknowledges this issue, stating, "Using the default NMK that is programmed into all AV stations. While this default NMK provides a seamless, Plug-and-Play experience for the user when the equipment is initially installed, it does not provide any privacy since it is known by every HPAV-certified station". This well-known NMK was previously exposed by Dudek [14] and Scholz [38]. In fact, it can easily be found by connecting to a Plug-and-Play PLC device through Ethernet with a computer and using the set of tools Open-PLC-Utils [36] suite to retrieve its NMK. This default Plug-and-Play



(a) $c = 1\,\text{m}$. (b) $c = 3\,\text{m}$. (c) $c = 5\,\text{m}$.

Figure 4.4: Scenario 1: A passive adversary wirelessly receives packets exchanged over the power line where the HomePlug packet rate is measured for each distance d between the system and the attacker, for each cable length c.

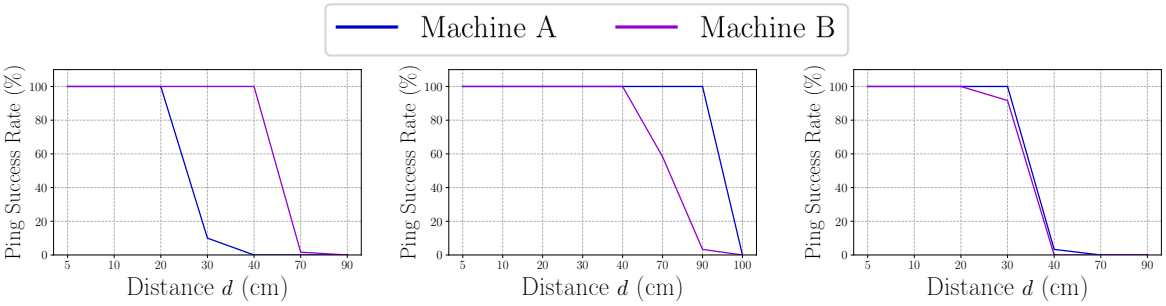
configuration allows attackers to perform more sophisticated attacks as they could easily join the victim's AVLN. Together with sniffing packets that can be intercepted on the power line, the attacker could demodulate encrypted packets destined to the AVLN legitimate stations or perform an active attack, which we explore in Scenario 2.

4.3 Scenario 2: Active Adversary, Bidirectional

4.3.1 Method

In this scenario, represented in Figure 4.3c, we assume that the adversary has managed to join the AVLN containing A and B. This assumption is reasonable, as evidenced by the results found in Section 4.2.3. The aim of this experiment is to evaluate the maximum distance at which the adversary could position themselves to perform active attacks, while being part of the target AVLN. This experiment also measures the maximum distance at which an adversary could perform their active attacks without being part of the AVLN, especially Denial-of-Service (DoS) attacks as presented in Section 2.4. Packet transmission does not depend on AVLN membership of the transmitting device, it is necessary only if we want to directly transmit to a device or network of devices from this AVLN. We give more insight on the first case (i.e., when the attacker has joined the AVLN) because it enables more impactful attacks.

Instead of sniffing for HomePlugAV packets like the previous scenario, the device $S2$ pings machine A and, in parallel, machine B with 64 B/sec of ICMP data bytes [27] for 60 seconds for each distance, for each cable length. We measure the success rate of this transmission, which implies



(a) $c = 1\,\text{m}$. (b) $c = 3\,\text{m}$. (c) $c = 5\,\text{m}$.

Figure 4.5: Scenario 2: An active adversary is part of the network and wirelessly transmits packets to other devices in the network, which are wired on the power line, where the ping success rate is measured for each distance d between the system and the attacker, for each cable length c.

the success of sending the packet, as well as receiving the confirmation that it was successfully transmitted, thus bidirectional. In order to be able to transmit properly, the amplifier was removed from the device for this scenario. $S1$ was kept to monitor HomePlugAV packets, including the ones transmitted by $S2$. This scenario represents an adversary who managed to join the AVLN and can now perform active attacks on the network.

4.3.2 Metrics

In Scenario 2, the adversary has joined the AVLN and actively participates in the network, transmitting data rather than passively sniffing. As such, the HomePlug packet rate is not as relevant as in the previous scenario. Instead, the transmission effectiveness is better captured by the Ping Success Rate, providing a direct indication of transmission quality. This rate is expressed as a percentage (%) and signifies the proportion of successful ICMP ping requests initiated by the adversary's device ($S2$) that receive a corresponding acknowledgment from the target devices (Machine A and B) within the network. Measuring the ping success rate for each distance and cable length lets us understand how far an adversary could position themselves to efficiently perform any active attack.

4.3.3 Results

In this scenario, the whip antenna did not prove useful as it was not able to transmit packets. For this reason, the results presented in Figure 4.5 were obtained solely using the dipole antenna. For all cable lengths, a full success rate could be achieved 20 cm away from the power line. Given that this distance is roughly equivalent to the thickness of a wall, it demonstrates that an attacker positioned on the opposite side of the wall containing the target power line could perform a full active attack.

Chapter 5

Real-World Testing

As the experimental setups are identical to the ones in Section 4.1, except for the shape and length of the power line connecting the two PLC devices, we chose the same metrics that were used previously to evaluate the results which allows for a proper comparison between the lab and real-world evaluation. For these experiments, we put in place a network of two domestic PLC devices in a building, where each device was connected via Ethernet to a machine, and each machine was communicating through PLC with the other one. As in most houses, the power line of the building was running in different rooms on different floors. We first executed a set of control experiments inside the building. Then, we performed experiments outside the building, in order to evaluate the maximum distance at which an attacker could position themselves outside of the victim's premises to achieve either Scenario 1 or Scenario 2. For better visualization, the setup for these experiments is illustrated in Figure 5.1. We split our evaluation in two scenarios.

5.1 Scenario 1

5.1.1 Method

In this case, we assumed an adversary who passively eavesdrops on the power-line communication in a real-world deployment. The attacking setup is identical to the setup described in Section 4.1 consisting of a HomePlug modem, which was set into sniffer mode. To improve the reception of the signal, an amplifier was connected to the input of the modem.

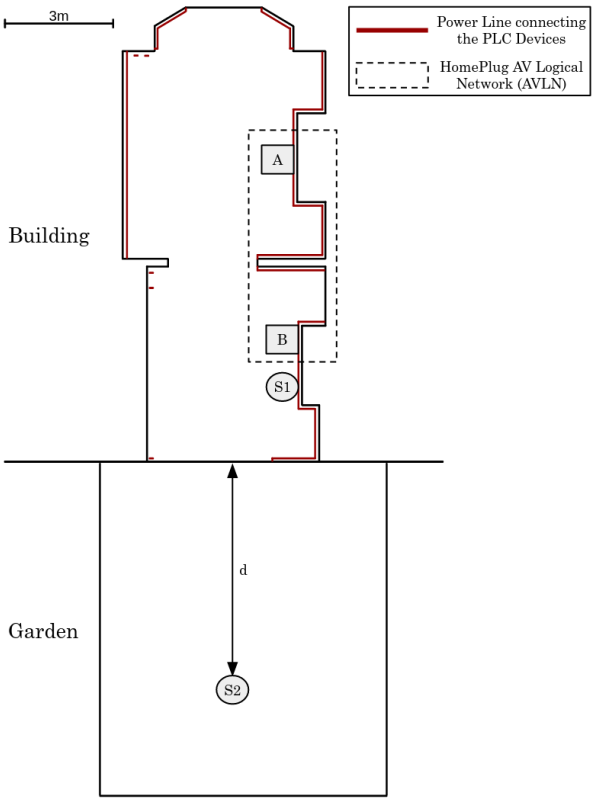


Figure 5.1: Illustration of the real-world experiment setup where PLC devices A, B and $S1$ are physically connected to the power line, with A and B being part of the same AVLN, and distance d between the external wall of the victim's building and the attacker $S2$.

5.1.2 Results

In this scenario, with the attacker inside the building, signal packet loss was limited to 300 packets (20% of the receiving rate on the power line): this is explained by the fact that, inside a building, increasing the distance from one wall inevitably decreases the distance to another one, which also contains power lines. While being an interesting result, it assumes that the attacker had access to the house of the victim. We want to evaluate if an outside adversary could attack the system and how far from the victim's house they could be.
In the context of evaluating an external attacker, the distance d becomes the distance between the external side of the wall of the target's building and the attacker's device. Figure 5.2 shows the result of real-world evaluation. With a whip antenna, an attacker could intercept about 1300 pkts/min (70 %) from just 1 m away, enabling discreet operation, potentially with the equipment concealed in a backpack while pacing near the victim's premises. The dipole antenna significantly boosted reception, capturing 1750 pkts/min of packets (92 %) from further away (i.e., 2 m). At a 4 m distance, the dipole antenna still managed to receive 200 pkts/min (11 %), indicating that attackers could operate from a distance, such as across the street, enhancing the feasibility of covert attacks.

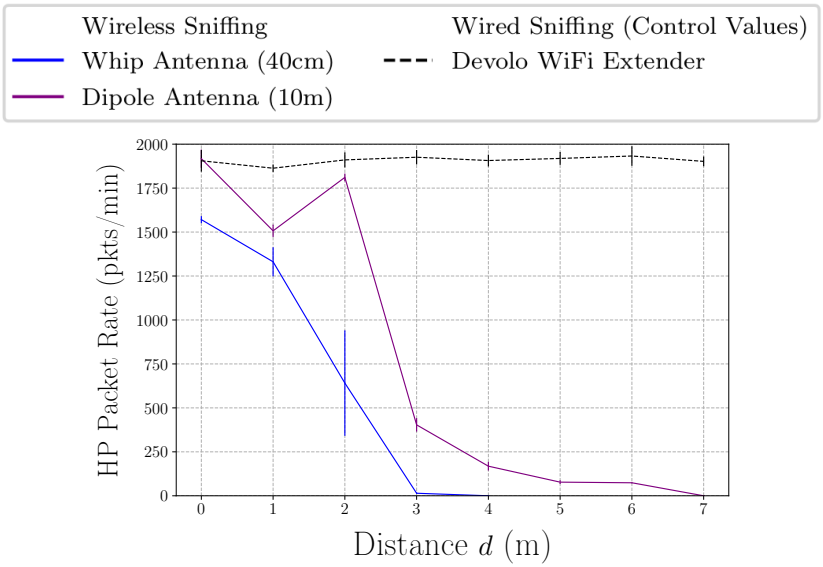


Figure 5.2: Real-World Scenario 1: A passive adversary wirelessly receives packets exchanged over the power line where the HomePlug packet rate is measured for each distance d between the external side of the wall of the target building and the attacker.

5.2 Scenario 2

5.2.1 Method

Building on the experimental framework discussed in Section 4.1, we assume an adversary has infiltrated the target network. In a real-world deployment, this active adversary repeatedly sends packets to each device within the network. The attack setup mimics the conditions of Scenario 2 in our lab evaluation, utilizing a HomePlug modem which has gained access to the victim's AVLN.

5.2.2 Results

Similarly to Scenario 1, we first performed the active attack within the building. As expected, we could achieve 100 % Ping success rate from anywhere within the building, as we would always be close to some power line.

Then, we tested this same attack outside of the building where, once again, d becomes the distance between the external side of the wall containing the power line and the attacker's device. Figure 5.3 shows the results. They were obtained solely using the dipole antenna: the whip antenna could not transmit a single packet to any of the two targeted machines. It is significant that a Ping success rate of 100 % is still achieved while transmitting to both machines for a distance of 50 cm

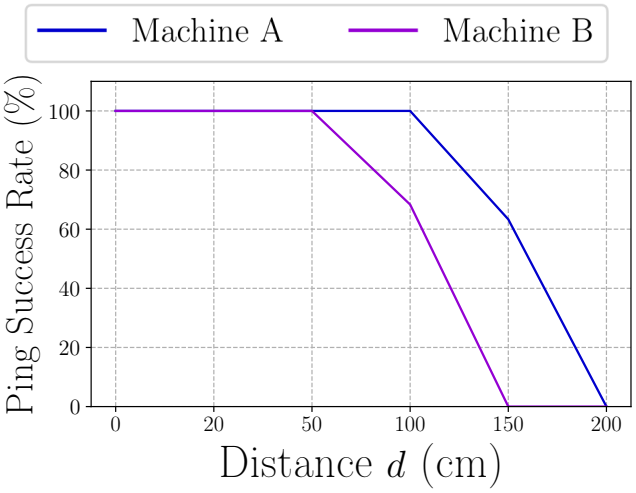


Figure 5.3: Real-World Scenario 2: An active adversary is part of the AVLN and wirelessly transmits packets to other devices in the network, which are connected via power lines. The ping success rate is measured for each distance d between the external side of the wall of the target building and the attacker.

from the wall and up to 1 m when sacrificing a perfect transmission rate for one of the machines. At 1.5 m, we were able to transmit efficiently to one of the machines, with a 65 % success rate. After that distance, the decreasing curve is quite steep as we experienced full packet loss, for each machine, at a 2 m distance.

Chapter 6

Discussion

6.1 Improving the Security of HomePlug

Given the inherent characteristics of the HomePlug PLC technology, without a significant change to the physical layer, the EM radiation is difficult to suppress. As such, to improve the security of PLC deployments without such changes, we explain and recommend the following optimizations:

Random Default NMK: As we have seen, almost all manufacturers continue to ship their PLC adapters with the default NMK to ease deployment and provide Plug-and-Play functionality. We argue, that since PLC adapters are usually sold in pairs, a random NMK can be installed in both adapters during the manufacturing process. This would substantially increase the security of PLC deployments, making it necessary to brute-force the NMK.

Malicious Device Detection: By default, PLC modems periodically transmit beacon frames. These frames can be observed by other HomePlug devices in sniffer mode. To detect the presence of unwanted devices in the AVLN, a legitimate modem in sniffer mode could be used to collect all MAC addresses of PLC devices and raise an alarm if unrecognized MAC addresses are detected. We acknowledge that a more sophisticated adversary might be capable of modifying their hardware to prevent the transmission of periodic beacons or spoof unique identifiers, such as the MAC address. However, the proposed solution significantly increases the necessary capabilities and entry barrier for an attack, potentially rendering it impractical or not worth pursuing.

Dummy Traffic for Privacy Protection: When considering an Honest-but-Curious adversary, or even a malicious adversary, eavesdropping on some PLC network traffic can lead to revealing sensitive user data and activities. The exchange of packets associated with data transmission (e.g., Start-of-Frame packets) becomes a potential source of information leakage as one could infer the

victim's behavior with tailored packet analysis (e.g., deducing the presence of the victim from peak activity in HomePlug traffic).

In response, we propose the introduction of dummy traffic in the AVLN. This strategy involves injecting dummy packets, which have the characteristics of standard data transmission packets, into the network. Despite the intentional discarding of these dummy packets upon reaching network devices, their transit through the network makes the countermeasure efficient. In the presence of a passive adversary engaged in traffic sniffing, the traversal of dummy packets prevents their ability to detect peaks in user activity. It hides the normal patterns of data exchange and confuses adversaries attempting to glean insights into victim behavior from packet analysis. Supposing that the adversary eavesdrops on the victim's AVLN traffic using the sniffer mode of a PLC device, dummy packets with minimal content (i.e., mostly headers) can be used. The sniffer mode only provides partial packet information, making lightweight dummy traffic feasible without disrupting normal transmission. Additionally, introducing dummy packets with fake network topology details can mislead adversaries. Legitimate devices discard these packets, but malicious sniffers capture incomplete information, preventing the adversary from understanding the actual network layout.

All countermeasures and mitigation techniques mentioned above can be implemented without requiring heavy changes to the existing protocols and infrastructures, which makes them easier and less costly. Certainly, more drastic and heavy measures could be considered, like investigating methods to reduce the unintentional EM emissions associated with PLC technologies [24, 33]. Another approach could involve adjusting the shielding of electrical wires to contain EM leakage, albeit at the potential expense of extensive modifications to existing infrastructure. This would not only incur substantial costs but also jeopardize one of PLC primary advantages – its ease of implementation on the existing wiring infrastructure.

6.2 Limitations

The main limitation of our design is the lack of amplification when our device transmits messages. Amplification can be used for reception only when the outgoing beacons from the PLC modem of the device are attenuated to avoid breaking the amplifier. The device needs an additional circuit to amplify transmission: both reception and transmission are needed because we need to receive the responses of the system to our transmitted packets. However, such combined circuit is hard to implement. This reason explains why we have to maintain a limited distance to the system to perform active attacks. The transmission power of our device is too low to send packets that reach the victim's system from a larger distance.

Another limitation is from the sniffer mode of PLC modems, as it does not fully demodulate packets and only reveals the header information of some HomePlug packets. Its main advantage is that the demodulation process is fast and allows for live attacks, even if offering only a section of the

complete information of each packet. Another approach to fully demodulate packets was taken by Baker et al. [3] where the HomePlug packets were captured and demodulated through a long receiver chain to recover messages, only after capture was over, because of heavy signal processing induced. This makes the attack only executable offline. It would be interesting to understand how one could expand the sniffer mode on PLC device to demodulate the full packets, as it would allow for powerful attacks to be performed live. A skilful attacker could modify the software of a PLC modem to force the demodulation of the whole packet. For ethical reasons, we decided not to develop such a tool that could be misused by others.

Another limitation of our research lies in one of the assumptions that was made. Our assumption relies on the premise that power lines are situated along the exterior wall of the victim's house. While this condition is not strictly necessarily, it significantly enhances signal reception for an external adversary. We consider this assumption reasonable, given that the majority of houses and apartments feature exterior lighting near the entrance door or a wall adjacent to the street.

It is important to note that none of the above-mentioned limitations are fundamental physical limitations. There does not exist a specific defined distance at which the adversary will never be able to perform their attack. It depends on the hardware used (e.g., amount of amplification) and the resources that an adversary is willing to invest in.

Chapter 7

Future Work

Amplification on Tx: The first addition proposed for this research involves addressing the lack of signal amplification during transmission. This can be realized through the integration of an amplifier into the device's transmission module. The amplifier's role is to magnify a radio frequency signal into a higher power signal [9], which makes the signal easier to intercept by the targeted machines. However, it is important to design an appropriate circuit that allows for amplification during the reception phase as well, thereby ensuring the effective reception of responses from the queried machines.

PLC Fingerprinting: In our experiments, we measured the HomePlug packet rate to understand the wireless propagation of the PLC signals. This is a very broad metric, which contains many different types of HomePlug packets (e.g., Beacons for network topology discovery, Start-of-Frames for data transmission). In future research, we will analyze what an adversary's passive sniffer can capture and what information can be deduced from this data that might invade the victim's privacy. Similarly to Website Fingerprinting where an adversary can observe the traffic patterns between a victim and network to predict the website visited by the victim [7], one hypothesis is that an adversary could infer online activities of the victim, depending on the traffic patterns of the intercepted HomePlug communication. For example, if the victim is currently watching TV or browsing through a particular website which the attacker could recognize.

Chapter 8

Conclusion

This study aimed to evaluate the scale and security of Power-Line Communication (PLC) systems, with a focus on HomePlugAV devices. We have uncovered a significant expansion of the threat model against PLC, challenging the conventional belief that attacks required physical access to the power lines. By leveraging readily available commercial off-the-shelf hardware, wireless attacks on PLC systems were demonstrated, highlighting the vulnerability and lack of security of these widely used communication technologies.

We explored scenarios involving passive adversaries, focused on sniffing communication, and active adversaries, capable of bidirectional interaction (i.e., sending and receiving packets). The results revealed the feasibility of wireless attacks, previously wired only, emphasizing the need for robust security measures in PLC deployments. Real-world testing further validated these findings, providing insights into the potential impact and reach of wireless attacks on PLC networks. The findings suggest that the perceived security advantage of limited physical access to power lines is unfounded, as a wireless adversary can infiltrate a PLC network from a distance of up to 1.5 m from the victim's house outside walls using simple equipment, and eavesdrop on the communication 4 m away. Based on our findings, we propose practical countermeasures aimed at improving the security of PLC deployments, without necessitating extensive modifications to existing protocols and infrastructure. We mention several directions for future research including working on the amplification limitation through the integration of suitable circuits. Furthermore, exploring PLC fingerprinting techniques could show the potential for adversaries to infer user activities based on intercepted HomePlug communication patterns.

In conclusion, our research shows that simple and impactful wireless attacks can be performed on PLC networks and devices, even though PLC is a wired technology, used in various domains. Thus, it is essential to understand the vulnerabilities, how they can be exploited and develop countermeasures to improve the security of such technologies.

Bibliography

[1] devolo AG. *Devolo*. en. 2002. URL: https://www.devolo.global/ (visited on 12/05/2023).

[2] Richard Baker and Ivan Martinovic. "EMPower: Detecting Malicious Power Line Networks from EM Emissions". en. In: *ICT Systems Security and Privacy Protection*. Ed. by Lech Jan Janczewski and Mirosław Kutyłowski. Vol. 529. Series Title: IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2018, pp. 108–121. ISBN: 978-3-319-99827-5 978-3-319-99828-2. DOI: 10.1007/978-3-319-99828-2_8. URL: https://link.springer.com/10.1007/978-3-319-99828-2_8 (visited on 09/12/2023).

[3] Richard Baker and Ivan Martinovic. "Losing the Car Keys: Wireless {PHY-Layer} Insecurity in {EV} Charging". en. In: 2019, pp. 407–424. ISBN: 978-1-939133-06-9. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/baker (visited on 09/12/2023).

[4] Xavier Carcelle. *Power Line Communications in Practice*. en. Artech House, 2009. ISBN: 978-1-59693-336-1.

[5] David Cassidy, Gerald Holton, and James Rutherford. *Understanding Physics*. en. Google-Books-ID: a9ARBwAAQBAJ. Springer Science & Business Media, June 2006. ISBN: 978-0-387-21660-7.

[6] Wai Kai Chen. *The Electrical Engineering Handbook*. en. Google-Books-ID: qhHsSlazGrQC. Elsevier, Nov. 2004. ISBN: 978-0-08-047748-0.

[7] Giovanni Cherubin, Rob Jansen, and Carmela Troncoso. "Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World". en. In: 2022, pp. 753–770. ISBN: 978-1-939133-31-1. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/cherubin (visited on 02/12/2024).

[8] Konstantin Chterev. "Power Line Communication for Long-Distance Underwater Applications". In: Sept. 2023, pp. 917–928. ISBN: 978-981-9932-35-1. DOI: 10.1007/978-981-99-3236-8_74.

[9] Spectrum Control. *RF Amplifiers*. en. 2024. URL: https://info.spectrumcontrol.com/rf-amplifiers-va (visited on 02/05/2024).

[10] Naya Cunha, Breno Bispo, K. Ferreira, Gilson Alves, Gustavo Esteves, Emmanuel Santos, and Marco Rodrigues. “Communication in Hospital Environment Using Power Line Communications”. In: Jan. 2022, pp. 1451–1455. ISBN: 978-3-030-70600-5. DOI: 10.1007/978-3-030-70601-2_214.

[11] devolo. *dLAN 550 duo+ Powerline – Internet from the electrical socket | devolo*. en. 2024. URL: https://www.devolo.global/dlan-550-duo-powerline (visited on 02/02/2024).

[12] devolo. *dLAN Green PHY module*. en. 2024. URL: https://www.devolo.global/dlan-green-phy-eval-board-ii (visited on 02/02/2024).

[13] devolo. *Magic 2 WiFi Next*. en. Item No. 08619. 2023. URL: https://www.devolo.global/magic-2-wifi-next (visited on 11/30/2023).

[14] Sébastien Dudek. “HomePlugAV PLC: Practical attacks and backdooring”. In: *Netw. Anal.* (2015), p. 51. URL: https://penthertz.com/resources/NSC2014-HomePlugAV_attacks-Sebastien_Dudek.pdf (visited on 12/12/2023).

[15] Sébastien Dudek, Jean-Christophe Delaunay, and Vincent Fargues. *HomePlugPWN*. original-date: 2019-04-01T12:49:20Z. Oct. 2023. URL: https://github.com/FlUxIuS/HomePlugPWN (visited on 12/01/2023).

[16] Sébastien Dudek, Jean-Christophe Delaunay, and Vincent Fargues. “V2G Injector: Whispering to cars and charging units through the Power-Line”. en. In: (2019).

[17] Stefan Hoffmann, Jens Müller, Jörg Schwenk, and Gerd Bumiller. “Powerless Security: A Security Analysis of In-Home Power Line Communications Based on HomePlug AV2”. In: Aug. 2020, pp. 213–232. ISBN: 978-3-030-57877-0. DOI: 10.1007/978-3-030-57878-7_11.

[18] PowerLine Alliance HomePlug Inc. *HomePlug AV Specification*. 2014.

[19] PowerLine Alliance HomePlug Inc. *HomePlug GreenPHY Whitepaper*. 2010. URL: https://content.codico.com/fileadmin/media/download/datasheets/powerline-communication/plc-homeplug-green-phy/homeplug_green_phy_whitepaper.pdf (visited on 09/12/2023).

[20] Filip Hossner, Jozef Hallon, Milos Orgon, and Rastislav Róka. “Testing of Electromagnetic Compatibility of PLC Modems”. In: *International Journal of Engineering Research and Technology ISSN 2278-0181* 5 (Jan. 2016), pp. 830–836.

[21] IEEE. “IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications”. In: *IEEE Std 1901-2020 (Revision of IEEE Std 1901-2010)* (Jan. 2021). Conference Name: IEEE Std 1901-2020 (Revision of IEEE Std 1901-2010), pp. 1–1622. DOI: 10.1109/IEEESTD.2021.9329263. URL: https://ieeexplore.ieee.org/document/9329263 (visited on 11/30/2023).

[22] ISO/TC 22/SC 31. *ISO 15118-1:2019 - Road vehicles — Vehicle to grid communication interface*. en. June 2021. URL: https://www.iso.org/standard/69113.html (visited on 11/30/2023).

[23] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. "Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging". en. In: *Proceedings 2023 Network and Distributed System Security Symposium*. San Diego, CA, USA: Internet Society, 2023. ISBN: 978-1-891562-83-9. DOI: 10.14722/ndss.2023.23251. URL: https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_s251_paper.pdf (visited on 09/12/2023).

[24] N.V. Korovkin, E. Marthe, Farhad Rachidi, and E. Selina. "Mitigation of electromagnetic field radiated by PLC systems in indoor environment". In: *International Journal of Communication Systems* 16 (June 2003). DOI: 10.1002/dac.595.

[25] Lutz Lampe, Andrea Tonello, and Theo Swart. *Power line communications: Principles, standards and applications from multimedia to smart grid: Second edition*. Apr. 2016. ISBN: 978-1-118-67671-4.

[26] Haniph Latchman, Srinivas Katar, Larry Yonge, and Sherman Gavette. *Homeplug AV and IEEE 1901: A handbook for PLC designers and users*. Journal Abbreviation: Homeplug AV and IEEE 1901: A Handbook for PLC Designers and Users Pages: 346 Publication Title: Homeplug AV and IEEE 1901: A Handbook for PLC Designers and Users. Sept. 2013. ISBN: 978-0-470-41073-8. DOI: 10.1002/9781118527535.

[27] Linux. *ping(8) - Linux man page*. 2024. URL: https://linux.die.net/man/8/ping (visited on 02/02/2024).

[28] Hui Liu and Guoqing Li. "OFDM-Based Broadband Wireless Networks: Design and Optimization". In: (Mar. 2006), pp. i–xii. ISSN: 9780471723462. DOI: 10.1002/0471757195.fmatter.

[29] A. Majumder and James Caffery. "Power line communication: An overview". In: *Potentials, IEEE* 23 (Nov. 2004), pp. 4–8. DOI: 10.1109/MP.2004.1343222.

[30] Maged Marghany. "Principle theories of synthetic aperture radar". In: *Synthetic Aperture Radar Imaging Mechanism for Oil Spills*. Gulf Professional Publishing, Jan. 2020, pp. 127–150. ISBN: 978-0-12-818111-9. DOI: 10.1016/B978-0-12-818111-9.00008-2. URL: https://www.sciencedirect.com/science/article/pii/B9780128181119000082 (visited on 12/15/2023).

[31] Alfred J. Menezes, Jonathan Katz, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. en. Google-Books-ID: nSzoG72E93MC. CRC Press, Oct. 1996. ISBN: 978-1-4398-2191-6.

[32] NES. *Smart metering and power line communications for utilities*. en-ZA. July 2021. URL: https://www.smart-energy.com/industry-sectors/smart-grid/smart-metering-and-power-line-communications/ (visited on 02/05/2024).

[33] T.S. Pang, P.L. So, and K.Y. See. "Feasibility Study of a New Injection Method for EMI Reduction in Indoor Broadband PLC Networks". In: *Power Delivery, IEEE Transactions on* 25 (Nov. 2010), pp. 2392–2398. DOI: 10.1109/TPWRD.2010.2043123.

[34] Lukas Potisk, Jozef Hallon, Milos Orgon, and Radek Fujdiak. “Electromagnetic compatibility of PLC adapters for in-home/domestic networks”. In: *Journal of Electrical Engineering* 69 (Jan. 2018), pp. 79–84. DOI: 10.1515/jee-2018-0011.

[35] Axel Puppe, Jeroen Vanderauwera, and Dirk-Jan Bartels. *Research Project: HomePlug Security*. Tech. rep. Universiteit van Amsterdam, 2010.

[36] Inc. Qualcomm Atheros. *qca/open-plc-utils*. original-date: 2013-01-21T21:46:30Z. 2013. URL: https://github.com/qca/open-plc-utils (visited on 12/05/2023).

[37] Alexander D Ryer. *The Light Measurement Handbook*. en. 1997.

[38] Rouven Scholz and Christian Wressnegger. “Security Analysis of Devolo HomePlug Devices”. en. In: *Proceedings of the 12th European Workshop on Systems Security*. Dresden Germany: ACM, Mar. 2019, pp. 1–6. ISBN: 978-1-4503-6274-0. DOI: 10.1145/3301417.3312499. URL: https://dl.acm.org/doi/10.1145/3301417.3312499 (visited on 09/12/2023).

[39] Ben Tasker. *Vulnerability: Infiltrating a network via Powerline (HomePlugAV) adapt*. en. July 2014. URL: https://www.bentasker.co.uk/posts/documentation/security/282-infiltrating-a-network-via-powerline-homeplugav-adapters.html (visited on 02/23/2024).

[40] Group tcpdump. *tcpdump*. 1999. URL: https://www.tcpdump.org/ (visited on 02/07/2024).

[41] TPLink. *TL-PA4010 KIT - Powerline 600 Starter Kit, 1 Port*. en-gb. 2024. URL: https://www.tp-link.com/home-networking/powerline/tl-pa4010-kit/ (visited on 02/02/2024).

[42] Emmanuel Chukwunazor Uwaezuoke. *Analysis of Power Line Communication Network Vulnerabilities Using Cyber Security Techniques*. Tech. rep. University of Johannesburg, Apr. 2022. URL: https://ujcontent.uj.ac.za/esploro/outputs/graduate/Analysis-of-power-line-communication-network/9917907107691 (visited on 01/19/2024).

[43] Christina Vlachou and Sébastien Henri. *A Practical Guide to Power Line Communications*. May 2022. ISBN: 978-1-108-83548-0. DOI: 10.1017/9781108890823.

[44] WiGLE. *WiGLE: Wireless Network Mapping*. 2004. URL: https://www.wigle.net/ (visited on 12/04/2023).

Appendix A

Availability

Our evaluation source code is available at `https://github.com/ssloxford/mind_the_gap`. This GitHub repository contains the tools used, as well as the scripts written for our experimental setup and evaluation.