Powerline Connections

Joe Montroy

29 January 2025

In this paper I will discuss the function of power-line connections (PLC) also known as Ethernet over Power (EoP). I will give a brief history of the medium and the published standards which the devices follow. I will break down piece by piece how the individual stations store and map the network, communicate to other network devices, and travel through the link and physical network layers. I will discuss the optimization of data throughput with MIMO and OFDM along with the security methods set out by the standard bodies to ensure a secure and safe connection. I will finish off by discussing the drawbacks of PLC and give a final recap.

In the 1920s, power outlets were becoming a standard across U.S. homes. New technological innovations, such as vacuums, toasters, and radios, required dedicated power sockets. The wires that ran to these sockets during this time period are called “knob-and-tube” wires. They are composed of a single copper conductor, a cotton coat, and sometimes a rubber outer layer. As you can imagine, with the cotton coat, this form of wiring was highly combustible and would occasionally catch on fire under load. The wiring was created primarily to support indoor lighting but was retrofitted to support outlets. Modern wiring provides a higher volume of electricity in a safer manner. Cables are typically bundled and kept in a PVC casing to prevent fire hazards. These are the cables that you will find in 99% of homes today. With a later start in history, ethernet was not developed until 1973 in the Xerox Research Center by Robert Metcalf. This basic cable was a thin coax cable made with a copper core and rubber shielding that could carry up to 1 Mbps. In the modern day, the most common ethernet cables are Cat5 and Cat6 cables. These have multiple sets of twisted copper cable pairs with Cat6 delivering speeds up to 10 Gbps. The current peak of ethernet cables is Cat8 cables, which reach speeds of 40 Gbps, 40,000 times the speed of Robert Metcalf’s first cable.

There are two major standards bodies that have released standards for power line ethernet. The first being the HomePlug 1.0 released by the HomePlug Alliance in June 2001. The HomePlug alliance followed up the 1.0 by releasing their AV (audio & video) standard in 2005. This update bumped theoretical throughput from 14 Mbps to around 200Mbps. In December 2010 the IEEE built off of the established AV1 and published its 1901-2010 standard. This paper became the new bar for powerline connection and named The HomePlug Alliance the certification body for powerline devices. In 2014, the Alliance modernized their AV1 standards to their new AV2 standard once again updating PLC for modern speeds. In 2016 the Alliance disbanded and placed all their documentation into the public domain. Following this in 2021, the IEEE released an updated 1901-2020 which is the most up to date standard for the medium. With the HomePlug Alliance gone, there are no official IEEE certification bodies for powerline adapters but most adapters today are marked as being up to AV2 standard or the 1901 standard.

Sending ethernet over power cables is achieved by sending the data at a frequency that does not interfere with the AC power. According to the IEEE 1901 the frequencies that powerline connections can run at are between 1.705MHz and 100MHz wherein typical AC power only runs at a frequency of 50-60 hz. At-home PLC systems use two or more adapters that plug into AC outlets. One adapter must be wired directly into the network router, while others can be placed anywhere on the same power grid. The speed of the connection over the powerline is dependent on the distance the signal has to travel and the amount of interference it encounters. Typical interference can come from breaker switches, strong RF signals, or power heavy appliances. Companies such as TP-link are currently the leaders in home PLC adapters; their TP-PA9020P model is rated at up to 2 Gbps. Although, the technology has come a long way since it was first introduced into the consumer market 25 years ago. Intellion pioneered the at-home industry with the introduction of its PowerPackets that boasted blazing speeds of 14Mbps.

When setting up a PLC system, two adapters or stations ("STAs") are plugged into the wall. The STA plugged directly into the router has what is called a "Basic Services Set Manager" (BM), which controls the basic operations for communication. To begin the setup of the network, the BM sends a discovery beacon out on the power grid in search of the endpoint STA. This beacon contains "information including the NID of the network, the TEI, the MAC address, and the number of discovered STAs and networks, and the BM capability of the transmitting STA." (IEEE 1901-2020, p. 664). Each STA will take this information and enter it into a "Discovered STAs" table and a "Discovered Networks" table. The Discovered STA table stores MAC addresses, a "same network" flag bit, and the short network NID tied to every STA the system comes across. The Discovered Networks table stores information about any NID of a beacon that is not on the same network. For example, if the power lines of an apartment building are all connected to the same grid, an STA's beacons could discover other networks along the grid that do not share its network. That STA would then log the NID of said discovered networks into its table.

After the BM has beaconed another STA on the network, it begins the process of channel estimation. Initial channel estimation is activated when the BM does not have any tone maps to the desired destination. To initialize a new map, the transmitter will send sound-MPDUs to the receiving STA. Sounding - MAC Protocol Data Units (MPDUs) measure channels for speed and response time by testing how long ACKs take to bounce back from the receiving STA. With the information gathered from sounding and response times, the BM can create a default tone map of the AC power line. With its initial map, the system begins the next phase of channel estimation known as dynamic channel estimation. “Once the initial channel estimation is complete, the receiver continuously monitors the channel characteristics based on received MPDUs (either data or sound) and provides dynamic updates to the default tone map and/or to the tone maps that are valid at specific intervals of the AC line cycle.” (IEEE 1901-2020 p. 619). Through the process of channel estimation the BM is able to constantly maintain a tone map of the AC power network and monitor it for the fastest routes to desired destinations.

Since BM has found the optimal route to the endpoint STA, connections are ready to be made. As the connection is being sent from the router to the STA to the wire, it passes through the link layer and the physical layer. The physical layer (PHY) controls operations such as error-correction, mapping, and STA level operations. The link layer or MAC Layer, controls the correct position of transmission, formatting of data frames, and error free delivery of packets through replay requests. Each of these layers communicate to each other through service access points (SAP) which act as bridges for information. When a connection needs to be sent over the powerline, the MAC layer will receive a MAC Service Data Units (MSDU) which contain the connection data. Before The MAC layer can send this data to the Physical layer, the MSDUs will go through what is called the MAC framing process. The framing process for MSDUs changes based on whether their data is labeled as connection or connectionless. Frame generation for connection MSDUs is rudimentary, as their data is simply pushed into an MSDU payload and gathered into an MPDU. For connectionless MSDUs the process requires more steps. The unit will either become a management frame or an MSDU payload. Management MSDU frames take the management payload and convert it into a compiled MAC frame. To create connectionless MSDU frames the system appends a MAC frame header and an integrity check value to the frame along with the original MSDU payload. Both frames are loaded into MPDUs and sent through the SAP to the physical layer for them to continue to the next step in the process.

Connections between STAs are made using Multi-In Multi-Out (MIMO) Orthogonal Frequency Division Multiplexing (OFDM). The AV2 standard for OFDM "employs up to 3455 carriers, in the range from 1.80 MHz to 86.13 MHz. Support for carriers above 30 MHz is optional." (HomePlug Alliance p.72) In early PLC systems OFDM was the only method utilized to speed up network transfers over the wire. It works by spreading the data along orthogonal subcarriers, sending little pieces of information on each one. This achieves a few things, one, it gives the system higher data throughput. Two, there is less interference between frequencies and decreases frequency fading. Three, retransmission of signals is made easier if data is lost. The early systems that are laid out in IEEE 1901-2010 use Single-In Single-Out (SISO) networking where the system would have one transmit signal path and one receiving signal path. In the new IEEE 1901-2020 PLC adapters use MIMO networking to connect across the network. MIMO networking utilizes two transmission paths and two receiving signal paths. Its operation is mainly run by the MIMO Parser who splits data and decides which transmit path it will travel along. The parser sends data in two separate types of beamforms. The first is Eigen Beamforming, this is the standard MIMO operation of splitting the data transmission among two different ports. The second is Spot Beamforming. This method takes a single data stream that is either phase shifted or scaled and transmits them on both ports. Eigen Beamforming is the faster method but Spot beamforming is better for data assurance.

A critical concern for powerline connections is the security of the data. In settings such as apartment buildings where power lines can be shared, how can these systems ensure the confidentiality of their data? The standard for systems outlined in the AV2 standard is to use

128-bit AES encryption keypairs that are either machine generated or based on pass phrases. Each STA has a specific device access key (DAK) that it receives from the manufacturer when built. Messages sent to a particular STA will be encrypted with its DAK, making it only accessible to the correct STA. An important piece of security for devices in the network is the Network Membership Keys (NMKs). NMKs are how STAs ensure the authenticity of other devices on the network and prevent a scenario of a malicious STA plugging in and immediately connecting. STAs are given access to NMKs when they are manually configured onto a network with its network password.

While being an underutilized and revolutionary idea, power line connections do have drawbacks. Firstly, realized speeds do not compare to those of modern ethernet capabilities. While companies such as TP-Link boast speeds of up to 2 Gbps, the realized speed ,according to most reviews, range around 200 - 500 Mbps. Secondly, the connection is reduced when the endpoint STA is a far distance from the receiver. Lastly, setting up power line networks is hard to plan for as an average consumer. Consumers who live in a house or apartment may not know the specifics of the wiring in said homestead to ensure a fast connection with minimal interference.

To recap, In this paper I discussed the function of power-line connections (PLC) and the frequencies they run at. I gave a brief history of the medium and the IEEE and HomePlug standards which the devices follow. I broke down piece by piece how STAs beacon to other devices on the network, send sound-MPDUs for channel estimation, and move data through the link and physical layer. I also discussed how OFDM and MIMO play in the optimization of the data over wire. Finally I discussed the security methods used by the standard bodies to ensure network security. While power line connection is a slowly dying medium due to unreliability and low speeds. It's one that captured my attention as a thoughtful unorthodox solution to networking.

Sources:

"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)* , vol., no., pp.1-1622, 19 Jan. 2021, doi: 10.1109/IEEESTD.2021.9329263.

HomePlug Powerline Alliance. *HomePlug AV Specification* Version 2.1, 21 Feb. 2014.

J. Lopes, J. P. Planells and A. Verl, "Real-Time Ethernet over Power Line," *2018 25th International Conference on Mechatronics and Machine Vision in Practice (M2VIP)*, Stuttgart, Germany, 2018, pp. 1-6, doi: 10.1109/M2VIP.2018.8600908.

Tyson, Jeff. *"How Power-Line Networking Works." HowStuffWorks*, 30 Apr. 2001, https://computer.howstuffworks.com/power-network.htm. Accessed 25 Jan. 2026

Irei, Alissa, and Eamon McCarthy Earls. "Understanding the Evolution of Ethernet." *TechTarget*, 25 Nov. 2019, https://www.techtarget.com/searchnetworking/feature/Understanding-the-evolution-of-Ethernet.

Techquickie. *How Does Powerline Ethernet Work?* YouTube, 21 Nov. 2017, https://www.youtube.com/watch?v=ywQeJCa3jl8.

International Association of Certified Home Inspectors. *“Knob-and-Tube Wiring.”* InterNACHI, https://www.nachi.org/knob-and-tube.htm. Accessed 23 Jan. 2026.