The Future of Transmission Protocols in the Context of a Smart Home System

Florian Brunen, Bastian Hodapp, Aljosha Vieth and Valentin Weber
Department of Computer Science
Furtwangen University of Applied Science
Furtwangen im Schwarzwald, Germany
{brunenfl, hodappba, viethalj, weberval}@hs-furtwangen.de

***Abstract*—What transmission protocols are available in the Smart Home space? How could this change in the foreseeable future? In this paper, we will discuss existing and emergent technologies, as well as evaluate how the recently developed Matter standard could affect the current market. We will show an overview of the Smart Home Lab of Furtwangen University as an example of a contemporary Smart Home and compare new technologies to those currently in use there.**

***Index Terms*—Smart Home, IoT, Matter, ZigBee, Wireless Communication**

I. Introduction

From 2020 to 2025, the amount of Smart Home technology that is being used in German households is estimated to roughly quadruple. Around 20 million households are expected to use Smart Home technology to control their lights, while 12.2 million households are expected to be using Smart Home security devices to secure their buildings [1].

While in 2021, the amount of Smart Home households was estimated to be about 10.49 million, the number is expected to rise to about double that number, 18.45 million, in 2025 [2].

The revenue generated by the Smart Home market in 2022 was around EUR 6.14 million. In 2027, this value is expected to about double to EUR 11.38 million [3].

This makes the Smart Home market one of the strongest-growing technology markets currently.

As more and more people are automating parts of their homes using Internet of Things (IoT) technology, the question of how these devices can communicate grows more important. Many manufacturers release devices that only work within their given ecosystems, much to the dismay of their users, who would like to buy devices and have them work with any other device. This challenge is on the horizon for Smart Home users and manufacturers alike, as there is a unified standard that would need to be implemented.

The new Smart Home standard Matter promises to provide a solution to this segregation of ecosystems by unifying the way in which devices are connected and how they can be accessed [4].

This paper provides an overview and comparison of a selection of existing Smart Home communication protocols and then compares them to the new Matter standard to evaluate if it can succeed in its goal to unify the Smart Home ecosystem.

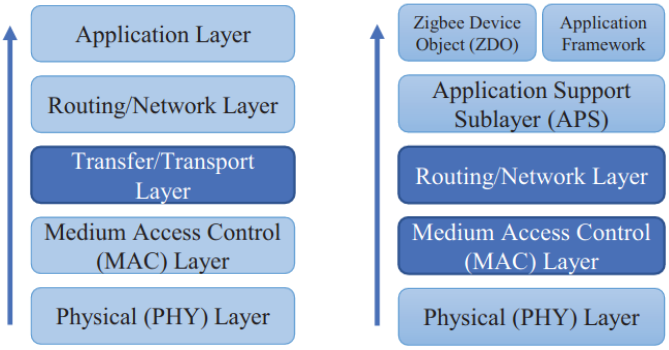
II. Background

In this section, we will discuss the technical background and attempt to define a state-of-the-art. We will briefly summarize the different technologies in use today and show their advantages as well as their shortcomings. We will focus almost exclusively on wireless technologies since there are only two prevalent protocols used over cables, Ethernet and KNX. Ethernet is a well-established standard, KNX will be discussed further in this section. The ISO/OSI model, initially drafted and standardized by the International Telecomunication Union (ITU) as ITU-T X.200, defines 7 layers [5]. For successful communication between two Smart Home devices, the interfaces/protocols of all of those layers need to be compatible.

As Smart Home systems are very dynamic and in general not very well engineered before deployment, the compatibility of communication protocol stacks between Smart Home system participants is even more important. In IoT applications other than Smart Home systems, systems engineering is heavily practiced prior to deployment, so these limitations only apply to the very specific field of Smart Home systems.

Although there are a lot of protocol stacks available for the different Smart Home use cases, many platforms and some associated protocols are owned by manufacturers and not publicly documented, rather than being open source. In some cases, this means there is no documentation publicly available and in many cases, this means there are no studies available on the compatibility of these platforms. Some examples of this include Apple's HomeKit [6] and Google Home [7]. The only way these devices can currently achieve interoperability with devices of other vendors is by using an open protocol, such as Universal Plug and Play (UPnP), Zigbee, or HTTP. If a device does not support any of the open protocols, it can only communicate with devices of the same vendor, using a Vendor Specific Protocol (VSP).

Another challenge in defining the state of the art is the lack of information about device or protocol usage. While there is some information found in the context of Industrial Internet of Things (IIoT), where a company may have published research, no such sources are available for the Smart Home context. As such, we are reliant on expert opinions and design papers, which propose the use of one technology in a scenario designed around specific use cases.



(a) Z-Wave Network Stack (b) Zigbee Network Stack

Fig. 1. Representation of the Z-Wave and Zigbee network stacks [8]

A. Z-Wave

While Z-Wave uses its own network stack, this stack looks similar to the traditional ISO/OSI model of network layers as defined by the ISO/IEC 7498 standard. This similarity becomes apparent when visualized in Figure 1a by Babun et al. [8]. The main difference is that Z-Wave omits the Session and Presentation layers present in ISO/IEC 7498, moving parts of the functionality to different layers and not using others.

Z-Wave builds a wireless mesh network topology, with each non-battery-powered device functioning as a relay node. This makes the network very resilient since any one node can fail without impacting other connections. This is different if the uplink fails, but the same is true for any other network.

Z-Wave communicates exclusively in the 900 MHz band, with a range of up to 30 meters [9]. This can be seen as an advantage since it means there is no possibility of interfering with other commonly used frequencies like 2.4 GHz. Furthermore, Z-Wave is a low power consumption transmission, which makes it well suited for a use-case like the Smart Home, in which devices powered by batteries or Power over Ethernet (PoE) are commonplace.

B. Zigbee

Zigbee is a wireless communication protocol that is based on the IEEE 802.15.4 standard for Wireless Personal Area Networks (WPANs) [10]. It defines its own physical and addressing layer (compare Figure 1b) and is the quasi-successor to Z-Wave. It was specifically developed for short to medium ranged networks with low power usage. It was designed to be compatible with a wide range of devices, from so-called smart bulbs to Zigbee routers.

The devices in a Zigbee network connect to each other and communicate in ad-hoc and static mesh networks. Each node with sufficient power can serve as a relay for new devices to connect to the network, similar to Z-Wave. A hub or gateway is needed to communicate with devices over other protocols. Zigbee operates in the 2.4 GHz band.

Zigbee used to be developed and promoted by an industry group called Zigbee Alliance. In the meantime, the Zigbee Alliance has become the Connectivity Standards Alliance (CSA) [11], which continues these tasks from now on.

In the Smart Home, Zigbee has become widespread through the support of vendors like IKEA and Philips Hue, who both use the protocol for their devices [12] [13]. Philips Hue, as well as IKEA, use the ZigBee Light Link standard, making their products mostly uncontrollable by ZigBee bridges of other manufacturers.

C. Wi-Fi

Wi-Fi is a standardized wireless networking technology that utilizes Radio Frequency (RF) waves in the 2.4 GHz and 5 GHz frequency bands to provide wireless high-speed Internet and network connections. The name Wi-Fi is a trademark of the Wi-Fi Alliance. The underlying technology is based on the IEEE 802.11 standard, which defines the specifications for wireless local area networks (WLANs) [14].

The operation of Wi-Fi technology is based on the use of Access Points (APs), which act as a bridge between wireless devices and the wired network infrastructure. These APs emit RF signals that can be received by Wi-Fi-enabled devices, such as laptops, smartphones, and Smart Home devices, within its range. This allows these devices to connect to the Internet and other network resources connected to the AP.

In terms of data transfer rates, Wi-Fi networks can provide speeds of up to several gigabits per second, which is sufficient for most Internet and network activities such as web browsing, streaming media, and file transfer. The range of Wi-Fi networks can be extended by the use of wireless repeaters or mesh network devices, which amplify the RF signals emitted by the APs.

Overall, Wi-Fi technology has become a ubiquitous means of providing wireless Internet and network access, and it is widely used in homes, offices, public spaces, and mobile devices. While in 2016, 8.36 billion devices worldwide were connected via Wi-Fi, this number was predicted to almost triple to 22.2 billion in 2021 [15]. In 2017, in Germany, about 95% of people used their own Wi-Fi network or share it with others [16]. Its widespread availability and compatibility with a wide range of devices have made it an essential aspect of modern communication and information technology.

In the Smart Home context, Wi-Fi is particularly useful for battery-powered devices or devices in hard-to-reach places such as light bulbs, as connecting them to the network via cable is often not possible. However, other protocols designed for low-power devices may do the job better. This means it is interchangeable with most other wireless connection standards, although the ubiquitous use of Wi-Fi for home networks means it is often the starting point.

It is important to note that Wi-Fi does not provide a standardized protocol, but merely the networking technology. This results in a wide variety of protocols using it as a base, but it is not sufficient to run a Smart Home. The most common protocol used over Wi-Fi is Internet Protocol (IP).

D. 6LoWPAN

IPv6 over Low power Wireless Personal Area Network (6LoWPAN) is a technology standard that enables the communication of Internet Protocol Version 6 (IPv6) packets over low-power wireless networks, specifically those based on the IEEE 802.15.4 standard. This allows for the use of IPv6-based networks in environments where low-power and low-data-rate devices are present [17].

6LoWPAN is an adaptation layer that sits between the IPv6 network layer and the IEEE 802.15.4 link layer. It is responsible for providing a mapping between the IPv6 packet header and the IEEE 802.15.4 frame format. This includes compressing the IPv6 header to reduce the size of the packet, as well as fragmentation and reassembly of packets to fit within the limited Maximum Transmission Unit (MTU) of the IEEE 802.15.4 link layer.

6LoWPAN also provides a number of additional features, such as addressing and routing, which are necessary for communication over the low-power wireless network. This includes the use of 16-bit short addresses for reduced overhead, as well as the use of multicast and anycast addressing for efficient communication.

Due to this efficiency, 6LoWPAN is widely used in the IoT and machine-to-machine (M2M) communication, as it enables the use of IPv6 networks in low-power, low-data-rate environments. This allows for the deployment of a wide range of devices, including sensors, actuators, and other low-power devices, in an IPv6-based network.

E. Bluetooth

Bluetooth is a wireless communication technology standard that operates in the 2.4 GHz Industrial, Scientific, and Medical (ISM) (Industrial, Scientific, and Medical) band. It utilizes short-wavelength Ultra High Frequency (UHF) radio waves to establish Personal Area Networkss (PANs) between fixed and mobile devices. It is a packet-based protocol, where data is divided into small packets, typically around 1,500 bytes in size, before being transmitted over the air. The technology uses a spread-spectrum, frequency-hopping technique, where the data is spread over a wide frequency band and the frequency of the transmission is rapidly changed in a pseudo-random manner. This allows multiple devices to communicate simultaneously over the same frequency band, reducing the likelihood of interference with other devices [18].

The technology uses a master-slave architecture, where one device acts as the master, while the other devices respond to the master's commands. The master device initiates the connection and controls the communication, while the slave devices respond to the master's commands.

Through the use of a modulation technique called Gaussian frequency-shift keying to encode the data before transmission, Bluetooth becomes less susceptible to interference. This technique uses a Gaussian filter to shape the frequency of the signal. In addition, Bluetooth also uses a technique called adaptive frequency-hopping to avoid interference from other devices that are operating in the same frequency band.

In the Smart Home context, Bluetooth is used to enable things like speakers communicating with a source of audio, as well as authentication and commissioning/onboarding of devices.

F. KNX

KNX, pronounced "Konnex", is one of the few wired communication protocols in the Smart Home space. It is an open standard, ISO/IEC 14543-3, and maintained by the KNX Association [19]. It evolved from three prior standards, the European Home Systems Protocol (EHS), BatiBus and European Installation Bus (EIB), which merged over time to form KNX as it is known today [20, p. 674]. It supports several types of cables, such as twisted pair, Ethernet, powerline, and radio for wireless communication [21]. When using KNX, there is no centralized control instance. Instead, the sensors send control commands directly to bus subscribers, such as smart bulbs or ventilation systems. Functions and assignments need to be manually configured with special software.

KNX differentiates between sensors and actuators. Sensors include all those you would typically see in a Smart Home, like temperature sensors, air quality sensors, and light sensors. Actuators are devices like light bulbs, Heating, Ventilation and Air Conditioning (HVAC) units, and motors controlling the blinds. Sensors generate commands, called telegrams, which then get directed towards the actuators, where functions turn them into actions [21].

The use of a bus system, rather than a classical network structure, allows a reduction in the amount of wiring needed. KNX uses a two-wire bus to communicate between sensors and actuators.

Despite being a good communication protocol for use in IoT applications, KNX has little practical application in the Smart Home space, due to the need to design the entire building around it. As far as residential buildings are concerned, cables are usually put in at the time of construction, and laying new cables comes with a significantly higher cost than adding wireless devices. While KNX does support radio in the 868.3 MHz band, in a purely wireless setup it cannot compete with protocols specifically designed for this. The radio support for KNX is meant to enable users to add singular devices that are not practical to connect by cable, not to build the entire network with it.

Therefore, while KNX is worth noting for industrial applications, we will not consider it further in this paper.

III. Definition of the context "Smart Home System"

A Smart Home is an interconnected and distributed system of IoT capable devices in a residential context [22].

These devices are meant to simplify everyday life and tasks, such as turning on/off lights or setting the heating temperature. The Smart Home system between those devices coordinates and controls them. It can perform tasks such as remote controlling lights, blinds and other devices as well as apply user-defined rules. Such rules can include turning off

lights and shutting blinds when everyone leaves the home, at night or with several other triggers.

A. HFU Smart Home Lab

We are using the Smart Home lab of the Hochschule Furtwangen University (HFU) as a reference point for our observations. The Smart Home lab contains several IoT Smart Home devices to provide an exemplary display of how a contemporary Smart Home can look.

We conducted an expert interview with the person in charge of the Smart Home lab [23].

The HFU Smart Home Lab was founded in ca. 2017. It was created to experiment on several developments in the area of IoT, with a focus on supporting humans in their daily lives.

Their job is to help students realize projects in the context of the Smart Home Lab. They are also responsible for maintaining the existing devices there, as well as incorporating new arrivals into the system.

The Smart Home Lab uses devices from about 20 to 30 different manufacturers, which amounts to around 100 different devices that communicate in the network of the Lab's context. There exist several devices that were once installed that have had their cloud support cut by the vendor since then, rendering them effectively unusable.

As far as wireless communication standards are concerned, we were told that the Smart Home Lab mostly uses HomeMatic IP devices, which use the 868MHz frequency band in Germany.

There is still a lot of Z-Wave/Fibaro being used in the Smart Home Lab. According to the Smart Home Lab, vendors are still selling several Z-Wave products. However, there are not many gateways to connect Z-Wave end devices available for purchase anymore. ZigBee is the wireless communication standard that mostly succeeded Z-Wave in the Smart Home Lab. It is better in terms of energy consumption, the robustness of communication, speed, and security.

The Smart Home Lab utilizes a multi-controller setup, where multiple controllers from different manufacturers are used to control the devices.

OpenHAB is used in the Smart Home Lab to make devices of different manufacturers connect together. It uses several pieces of connector software, called bindings, to connect a plethora of different device classes and protocols. Examples of bindings are ones for MQTT, Bluetooth, Linux Shell scripts as well as HomeMatic, IKEA or Philips Hue. Using these Bindings, OpenHAB can talk to, control and get data from different kinds of Smart Home devices. This makes the network of the Smart Home Lab basically a tree-like structure with OpenHAB at its top, controlling everything. The price to pay for this interoperability is the amount of configuration that needs to be put into adding all the devices into OpenHAB. Most of the time, every single device needs to be configured manually.

Figure 2 visualizes this setup using Systems Modeling Language (SysML).

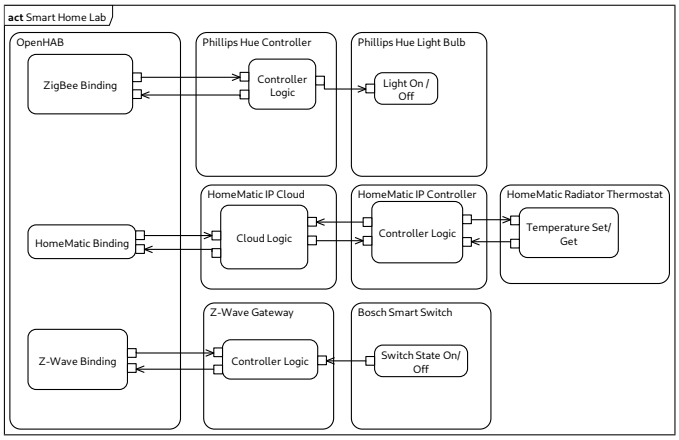


Fig. 2. Schematic, simplified SysML Representation of the HFU Smart Home Lab setup

OpenHAB communicates only with the controller/gateways for each manufacturer of Smart Home devices. It usually cannot directly control the actual devices, such as lightbulbs, blinds or sensors, but instead relies on communicating with these manufacturer-specific gateways. This leads to a lot of gateways that need to be bought if one wants to use products from different manufacturers. Sometimes, such Gateways also don't allow OpenHAB to control them directly, and instead need a cloud service to be available at all times for them to be controlled. This can lead to problems where cloud support gets cut from the manufacturer side, rendering the affected products effectively obsolete, even though their hardware would still be fine.

While there are devices that would not be able to be controlled by a system like OpenHAB at all, we were told that products are usually only considered to be bought for the Smart Home Lab if they will be supported by OpenHAB.

As far as the future of wireless communication protocols is concerned, Wi-Fi is the protocol that is most future-proof according to the Smart Home Lab. This is, according to them, because of the ubiquity of the protocol, since virtually everyone has a Wi-Fi router already in their home. Contrary to ZigBee and Z-Wave, they see no danger of Wi-Fi being abandoned in the short to mid-term future. the Smart Home Lab has not had any experience with Thread yet, because the last time devices were ordered, there were not many Thread devices available yet. However, the existing Z-Wave devices that are still in use in the Smart Home Lab will be replaced with ZigBee devices in the future.

B. Home automation software example: OpenHAB

A central Open Home Automation Bus (OpenHAB) server [24] is used to control various sub-controllers, which in turn are in charge of controlling various manufacturer and/or protocol-specific devices. This is achieved by utilizing multiple, manufacturer-specific bindings on the OpenHAB server [25]. In some cases, the sub-controllers are not directly

manageable by the OpenHAB server, but instead accessible via a cloud service.

Currently, it is very difficult to incorporate devices from various manufacturers into a single Smart Home setup without elaborate software like OpenHAB or Home Assistant that acts as a middleman to interconnect different protocols or devices.

This kind of "home automation software" is often difficult to set up and manage for the average user who just wants a single place to control all of their Smart Home devices. This is due to the fact that the devices and the way they are displayed in the OpenHAB user interface have to be defined by the user themselves [26]. There are some templates provided by the bindings for Smart Home devices in OpenHAB, for example [25], but it is still more manual work than most people are ready to invest.

IV. New transmission protocols

Although many manufacturers established their own protocols, which often limited incompatibility, efforts have been made in the recent past to develop a common path. This paper focuses on the recently released Matter standard and the Thread protocol that is used by it, alongside Wi-Fi.

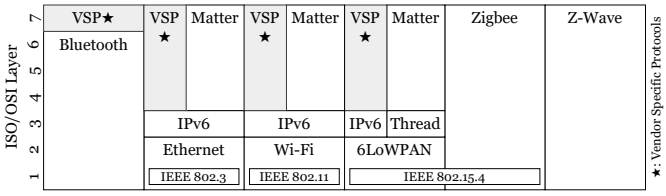


Fig. 3. Transmission Protocol Stacks

A. Thread

Thread is a comparatively new IoT protocol developed by Thread Group Inc. that got released in 2015. Thread is based on IEEE 802.15.4 and operates at 250 kbps in 2.4 GHz band [27]. IEEE 802.15.4 uses the two lowest layers of OSI and is used to define addressing and physical communication. The specific implementation of this standard that Thread uses is 6LoWPAN In Thread, six different types of devices exist, also visualized in figure 4:

Border Routers are used to connect the Thread network to other networks, e.g., Wi-Fi. There usually exist several Border Routers in a network and if the leader fails, a new one gets elected by the network.

Routers are used to provide routing services to other devices on the network, as well as to allow new devices to join the network.

Router Eligible End Devices (REEDs) are devices that are capable to act as a Router, however, they are not used as routers at the moment. They can be transformed into a Router if needed by the network and are always online.

Full End Devices (FEDs) are REEDs that are, for any reason, not capable of switching to routing mode at the moment.

Minimal End Devices (MEDs) are permanently online host devices and can only communicate through a Router. They are not capable of switching to routing mode. Messages can be sent to MEDs.

Sleepy End Devices (SEDs) are host devices, that only get online on a regular basis. Messages can not be pushed to SEDs, instead, they poll for new messages. They can not perform routing operations.

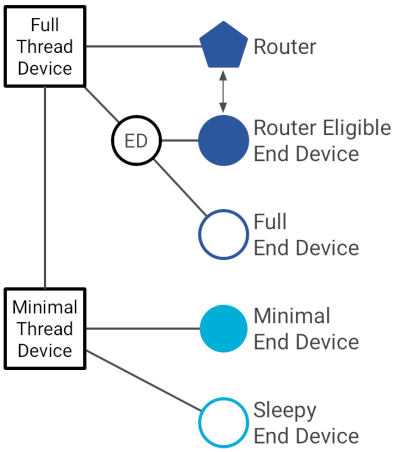


Fig. 4. Thread device types[28]

A key feature of Thread is the fact that it is designed to prevent single points of failure by virtue of its design as a mesh network with several REEDs. Although some Thread devices have special roles, they can be replaced on the go without impacting communication, as long as compatible devices exist in the network that can fill the gap (REEDs). An example of such an upgrade of a REED is shown in figure 5.

The only type of devices that cannot simply be replaced without impacting the network are Border Routers because there is not necessarily another Thread device in range capable of communicating with the other protocol.

B. Matter

Matter is an emerging IoT standard that was developed by the CSA and released on September 28, 2022 [29]. Matter is being co-developed by many companies in the Smart Home sector, including Amazon, Google, Apple, IKEA, Osram, Tuya

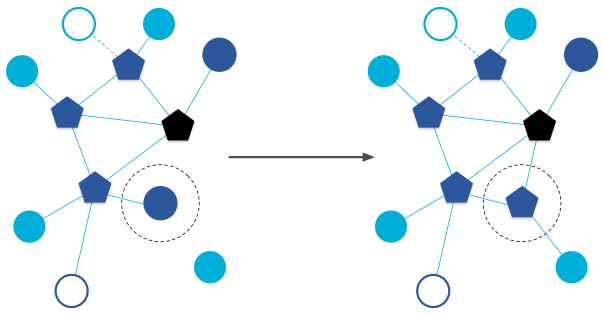


Fig. 5. Example of Thread router upgrade [28]

and Wulia [29]. Matter focuses on interoperability between devices from different manufacturers, which is ensured through cooperation between the companies. As long as manufacturers create devices compatible with Matter, they do not have to worry about interacting with the proprietary standards of different competitors. Matter itself is an open standard which enables everyone to use it for free.

Matter was designed to provide simplicity, interoperability, reliability, and security to users who want to connect their Smart Home devices with each other. Where multiple proprietary protocols from various manufacturers were needed before, Matter will be able to connect participating devices using a unified way of communication.

Matter supports the transport protocols Wi-Fi, Ethernet, and Thread for IoT device communication in its version 1.0. Bluetooth Low Energy (BLE) is supported for onboarding/commissioning of new devices. This simplifies device setup from, e.g., a smartphone app [4].

1) Protocol layers: Matter uses a layered architecture that encapsulates the pieces of the protocol stack [4, pp. 45–47]. The six layers from top to bottom are:

1) Application Layer: The main logic of a device, e.g., logic to control a lightbulb
2) Data Model: The Data Model defines the structure of the data used for the defined functionality of the device.
3) Interaction Model: The Interaction Model defines the interactions between client and server devices. The interactions refer to the elements from the data model.
4) Action Framing: The Action Framing layer serializes the actions from the Interaction Model into a packed binary format to use in network transmissions.
5) Security: The Security layer encrypts the serialized frames from the Action Framing layer. It also appends an authentication code to the message. This ensures authenticity and confidentiality between the parties.
6) Message Framing + Routing: This layer creates the final payload and adds optional header fields that describe the message.
7) IP Framing + Transport Management: This is responsible for the transport of the final message. The protocol is either the Message Reliability Protocol specified by Matter or TCP.

Once a message is received, it travels up the layers and gets deconstructed to be finally used by the application.

Matter does not prescribe exclusive network access or ownership. This means that several Matter networks can share the same IP network. [4, p. 47]. Matter also works without global routing IPv6 infrastructure, which enables the usage in a local network without an internet connection.

2) Network topology: In Matter, every device is represented as a node. Matter supports a so-called "single network topology" and a "star network topology". If all Matter devices are connected to one single logical network, e.g., a Thread network or a Wi-Fi network, that is an example of the single network topology. If several logical networks are used, e.g., a Thread network and a ZigBee network, it is called a star network topology. All networks are connected by one common hub network. This enables the integration of existing devices with older protocols, such as ZigBee, into the new standard [4, pp. 47–48]. This capability is important for customers, as it allows them to upgrade to the new standard and still use their old devices interoperatively. This makes the switch to Matter easier and prevents the need to replace devices that are actually still functional.

3) Addressing of Matter devices: Matter devices are collected in a so-called "Fabric" [4, p. 49]. A Matter network can have several Fabrics. Each node is addressed in the fabric via a "Node ID". Each Fabric is also identifiable by an ID. Matter devices can be part of several Fabrics, hence, having several IDs. In the end, "Node IDs" and "Fabric IDs" are mapped to IPv6 addresses.

4) Security: Matter uses public-key cryptography based on elliptic curve cryptography using the US National Institute of Standards and Technology (NIST) P256 curve [30], as well as digital signatures based on the same [4, p. 56]. Unicast messages between nodes provide replay protection and are secured and authenticated.

5) Sleepy End Devices: As specified in the Thread specification, Matter also supports so-called SEDs [4, p. 57]. The main goal is to extend the battery life of those devices. If it is a Thread device, it uses the functionality of SED devices specified by Thread. However, Matter also provides SED support for other protocols, like Wi-Fi. The basic behavior of SEDs is to deactivate the IP interface and the underlying technology (radio or link). It then wakes up periodically to communicate with the network. This feature enables a longer battery life for Wi-Fi devices, which are not designed for low power, and thus brings enormous added value.

6) Availability of devices: Since Matter is a new standard, there are few devices that support Matter yet. Some old devices will get updated to support Matter. However, a lot of manufacturers already announced new devices as seen at the Consumer Electronics Show (CES) in early 2023 [31].

V. What to use in the future?

It can be assumed that Matter will simplify a lot of things about the construction of a Smart Home system, as far as the near future is concerned. Customers need only pay attention to the "supports Matter" Logo on products to guarantee that a product they wish to buy is supported by their existing setup, should they already have implemented Matter.

There are only a few device classes supported for now [29], but those categories are specifically designated to be extended in the future.

As the Matter standard is open to everyone, there are no fees for anyone that wants to join. Developers can pick up the specification and start implementing it into their newer devices, ensuring them compatibility with other Matter devices.

What remains to be seen, however, is whether manufacturers will integrate Matter to work as well as their own proprietary networking technology. If they choose not to do so, but rather tack on Matter support as a bonus feature, we could see a

TABLE I
COMPARISON OF TRANSMISSION PROTOCOLS

Protocol	ISO/OSI Layer(s)	Frequency in MHz	Range in m	Transmission Power in mW	Enforces Encryption?	Meshable?
Z-Wave	1-7	850-950	40	1	Yes	Yes
Zigbee	1-7	868–868.6 & 2400–2483.5	10	1	Yes	Yes
KNXnet	1-7	N/A	N/A	N/A	No	N/A
Bluetooth	1-6	2402-2480	10-40	1	No	Yes
Matter	4-7	N/A	N/A	N/A	Yes	N/A
IPv6	3	N/A	N/A	N/A	No	N/A
Thread	3	N/A	N/A	N/A	Yes	N/A
Wi-Fi	1-2	2401–2473 & 5150–5815	15-45	100	No	Yes, but uncommon
6LoWPAN	1-2	868–868.6 & 2400–2483.5	10	1	No	Yes
Ethernet	1-2	N/A	N/A	N/A	No	N/A

situation akin to that of Apple smartphones and laptops. In that situation, while it is possible to operate the device in conjunction with devices of other manufacturers, doing so offers significantly lower quality than using only the devices of one company.

This problem is the main issue facing Matter, as it could easily turn customers away from shifting their existing system to using Matter. After all, users do not usually adopt new technologies without great incentive, similar to how Smart Home technology in general was adopted more slowly than originally anticipated [32]. As such, it can be assumed that Matter will need to be easy to integrate into an existing setup even for the less technologically literate user, as well as offer the same amount of features in order to become widely used.

A. Comparison of transmission protocols

As shown in table I, there are various differences between traditional and emerging transmission protocols. For Smart Home systems, the wireless range of devices is very important. As lower radio frequencies are better suited to pierce walls and obstacles, those are desirable. Secondly, a smaller transmission of power is desired, as devices in a Smart Home system are often placed remote and equipped with only a small battery. To increase the coverage of wireless networks, meshing is important. Additionally, as Smart Home systems are often used to control security-relevant parts of a house, encryption should be enforced by as many components of the stack as possible.

The use of VSPs lowers the probability that devices of different vendors are able to communicate with each other. However, as there are reasons for VSPs, the use of those is not uncommon. As publicly available documentation about VSP internals is not common, those are not considered for the remainder of this paper.

Examples for common stacks (consisting of ISO/OSI layers 1 to 7 [5]) are:

- Wi-Fi, IPv6, Matter: High power consumption at high range. Encryption is only enforced through the Matter protocol. Can be routed to the internet.
- 6LoWPAN, IPv6, Matter: Small power consumption at medium range. Encryption is only enforced through the Matter protocol. Can be routed to the internet.
- 6LoWPAN, Thread, Matter: Small power consumption at medium range. Encryption is enforced through the Thread and the Matter protocol.
- Wi-Fi, IPv6, VSP: High power consumption at high range. Can be routed to the internet. VSP lowers compatibility with devices from alien vendors.
- 6LoWPAN, Thread, VSP: Low power consumption at medium range. The VSPs, required on ISO/OSI layer 7, lowers compatibility with devices from alien vendors.
- Bluetooth, VSP: Low power consumption at medium range. The VSPs, required on ISO/OSI layer 7, lowers compatibility with devices from alien vendors.
- Z-Wave: Implements allISO/OSI layers and is therefore independent of VSPs. Z-Wave is a low-power, low-range protocol. The low range is extended through meshing, which is a key component of Z-Wave.
- Zigbee: Is traded as the unofficial successor to Z-Wave. It also is a low power, low range protocol, and also implements ISO/OSI layers 1 to 7. Other than Z-Wave, Zigbee is an openly developed standard by the CSA-IoT.

The problem of non-openly developed ISO/OSI layer implementations was already visualized in table 3.

B. Are OpenHAB and other Smart Home automation systems still needed?

OpenHAB and similar systems such as Home Assistant, Google Home, Apple HomeKit or other manufacturer-specific software will ideally only be needed as a means to interface the existing Smart Home system anymore, as Matter will make those systems obsolete in terms of setup and configuration of devices. Those systems might still be needed to manage Smart Home automation tasks such as shutting off the lights under specific circumstances, though, since Matter is only the protocol used to communicate with the devices and doesn't handle device behavior directly.

All of those assumptions are based on Matter gaining significant ground and being adopted by as many manufacturers as possible.

C. The Thread protocol

Since Matter is explicitly supporting the Thread protocol in its specification, it can be assumed that, should Matter become widely used, Thread's popularity will also increase. Contrary to Zigbee, Thread devices communicate using IPv6 addresses, which is required by the Matter protocol. Using IPv6 addressing also enables end devices to communicate with the globally routed internet more easily.

D. Existing and unsupported devices

While many big players have pledged to support Matter (at least on new devices), there is still the matter of older devices that use protocols that are not supported by Matter, such as Zigbee or Z-Wave. There are some proposals to handle those older devices by, for example, bridging their protocol to Matter with a kind of adapter layer. It is, however, still uncertain how well they will be supported, if at all.

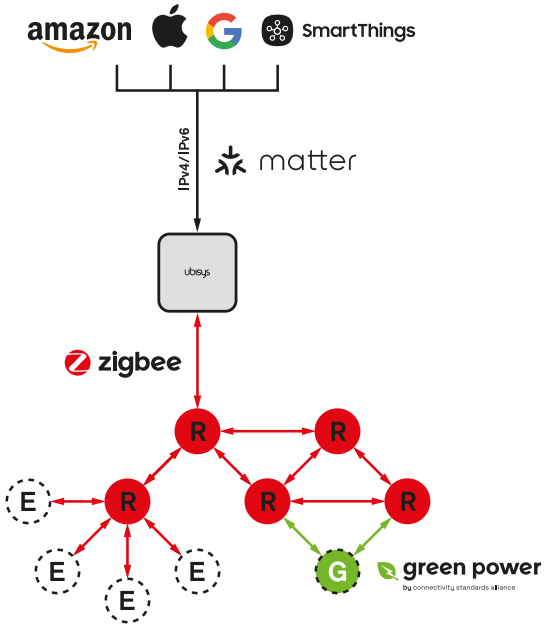


Fig. 6. Diagram of the ubisys Conflux gateway communication to the Matter stack [33]

The German manufacturer ubisys, for example, is planning to release a gateway that can address Zigbee devices over Matter [33]. As seen in Figure 6, Matter can address the ubisys Conflux hub via its IP-based protocol, which in turn forwards messages to its connected ZigBee devices.

In effect, this will be similar to how Thread border routers currently work.

VI. Application Example

Currently, if a new device is to be provisioned/onboarded to the existing setup in the Smart Home Lab, there are several steps that need to be taken. First, the device needs to be paired with the vendor-specific hub that is responsible for connecting said device to the IP-based network. Secondly, an OpenHAB binding must exist to connect the vendor-specific hub to the existing OpenHAB setup. Without such a binding, controlling the newly added device in conjunction with the other devices that have already been added to OpenHAB can be difficult to impossible.

A. Setup with Matter

With matter-enabled devices, the setup process is simplified. Since Matter provides a unified provisioning process for onboarding new devices, there is no need to look for apt bindings to interact with the existing ecosystem. The Matter protocol allows devices to talk to each other regardless of vendor or other factors. The only requirement is that the end devices as well as the routing devices in the network support the Matter protocol.

VII. Conclusions and Future Work

While Zigbee, Z-Wave and the other protocols mentioned in the paper offer a good solution for users who are content with a limited selection of manufacturers, the future of the Smart Home is likely to be a heterogeneous one. That way, users can take advantage of the individual benefits of each protocol, picking the best for their use case.

Matter is likely to provide a good interconnection between the many technologies currently in use. As we have shown, not all of these technologies are compatible for use with each other as of now, an issue that Matter was specifically designed to fix. With most of the big players in the Smart Home industry pledging to implement Matter support, there is a good chance Matter will become the new de facto standard.

The next step in continuing the work of this paper is only possible after waiting for Matter to either become established in the market or fail. After a few years, the results of this paper should be re-evaluated. Should Matter fail to establish itself, the work of this paper can also be built upon in postmortem analysis. In what we believe to be the more likely scenario, where Matter is widely adopted, the next step is to test different Smart Home network setups to find out which work best for different constraints like low power consumption.

References

[1] B. Mathias, *Infografik: So smart sind Deutschlands Haushalte — Statista*, May 2021. [Online]. Available: https://de.statista.com/infografik/3105/anzahl-der-smart-home-haushalte-in-deutschland/ (visited on 01/18/2023).

[2] Statista, *Smart Home - Anzahl der Haushalte in Deutschland 2025 — Statista*, Jun. 2021. [Online]. Available: https://de.statista.com/prognosen/885611/anzahl-der-smart-home-haushalte-in-deutschland (visited on 01/18/2023).

[3] Statista, *Smart Home - Deutschland — Statista Marktprognose*, Dec. 2022. [Online]. Available: https://de.statista.com/outlook/dmo/smart-home/deutschland (visited on 01/18/2023).

[4] Connectivity Standards Alliance, "Matter Specification," en. [Online]. Available: https://csa-iot.org/wp-content/uploads/2022/10/22-27349-001_Matter-1.0-Core-Specification76.pdf.

[5] ITU-T, "X.200 : Information technology - Open Systems Interconnection - Basic Reference Model: The basic model," Jul. 1994. [Online]. Available: https://www.itu.int/rec/T-REC-X.200-199407-I/en (visited on 01/19/2023).

[6] C. Vongchumyen, S. Torthitithum, J. Khamsopa, and P. Watanachaturaporn, "Home Appliances-Controlled Platform with HomeKit Application," in *2019 5th International Conference on Engineering, Applied Sciences and Technology (ICEAST)*, Jul. 2019, pp. 1–4. DOI: 10.1109/ICEAST.2019.8802605.

[7] *A home that knows how to help.* en. [Online]. Available: https://home.google.com/welcome/ (visited on 12/14/2022).

[8] L. Babun, H. Aksu, L. Ryan, K. Akkaya, E. S. Bentley, and A. S. Uluagac, "Z-IoT: Passive Device-class Fingerprinting of ZigBee and Z-Wave IoT Devices," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, ISSN: 1938-1883, Jun. 2020, pp. 1–7. DOI: 10.1109/ICC40277.2020.9149285.

[9] S. J. Danbatta and A. Varol, "Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2019, pp. 1–5. DOI: 10.1109/ISDFS.2019.8757472.

[10] The ZigBee Alliance, "ZigBee Specification."

[11] C. S. Alliance, *Our Members — Promoters — Participants — Adopters*, en-US, Oct. 2022. [Online]. Available: https://csa-iot.org/members/ (visited on 10/28/2022).

[12] IKEA, *Smarte Beleuchtung - Kompatibilität & Protokolle IKEA - IKEA Schweiz*. [Online]. Available: https://www.ikea.com/ch/de/customer-service/product-support/smart-lighting/kompatibilitaet-protokolle-pub3d9a0d29 (visited on 01/19/2023).

[13] Philips, *Hue Hue Bridge — Philips Hue DE*. [Online]. Available: https://www.philips-hue.com/de-de/p/hue-hue-bridge/8719514342620#features (visited on 01/19/2023).

[14] "IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pp. 1–4379, Feb. 2021, Conference Name: IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016). DOI: 10.1109/IEEESTD.2021.9363693.

[15] IDC, *WLAN connected devices worldwide 2016-2021 — Statista*, Dec. 2017. [Online]. Available: https://www.statista.com/statistics/802706/world-wlan-connected-device/ (visited on 01/20/2023).

[16] OnePoll, *WLAN - Form der WLAN-Nutzung in Deutschland im Jahr 2017 — Statista*, Jul. 2017. [Online]. Available: https://de.statista.com/statistik/daten/studie/733835/umfrage/umfrage-zur-form-der-wlan-nutzung/ (visited on 01/19/2023).

[17] G. Montenegro, C. Schumacher, and N. Kushalnagar, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," Internet Engineering Task Force, Request for Comments RFC 4919, Aug. 2007, Num Pages: 12. DOI: 10.17487/RFC4919. [Online]. Available: https://datatracker.ietf.org/doc/rfc4919 (visited on 01/19/2023).

[18] B. SIG, *Bluetooth Core Specification*, Jul. 2021. [Online]. Available: https://www.bluetooth.com/de/specifications/specs/core-specification-5-3/ (visited on 01/19/2023).

[19] *For Professionals – KNX Association [Official website]*. [Online]. Available: https://www.knx.org/knx-en/for-professionals/ (visited on 01/22/2023).

[20] M. Dehli, "Energieeffiziente Gebäudetechnik – Gebäudeautomation – Monitoringkonzepte beim Betrieb von Großgebäuden," de, in *Energieeffizienz in Industrie, Dienstleistung und Gewerbe: Energietechnische Optimierungskonzepte für Unternehmen*, M. Dehli, Ed., Wiesbaden: Springer Fachmedien, 2020, pp. 653–686, ISBN: 978-3-658-23204-7. DOI: 10.1007/978-3-658-23204-7_18. [Online]. Available: https://doi.org/10.1007/978-3-658-23204-7_18 (visited on 01/22/2023).

[21] WAGO, *KNX – Communication Protocol for Building Automation*, en-US. [Online]. Available: https://www.wago.com/us/knx (visited on 01/19/2023).

[22] Prof. Dr. Oliver Bendel, *Smart Home • Definition — Gabler Wirtschaftslexikon*. [Online]. Available: https://wirtschaftslexikon.gabler.de/definition/smart-home-54137 (visited on 01/19/2023).

[23] M. Dörflinger, *State of the HFU Smart Home Lab and possible future developments*, German, Nov. 2022.

[24] openHAB Foundation e.V., *openHAB*, 2023. [Online]. Available: https://www.openhab.org/ (visited on 01/18/2023).

[25] openHAB Foundation e.V., *Add-ons — openHAB*, 2023. [Online]. Available: https://next.openhab.org/addons/ (visited on 01/18/2023).

[26] openHAB Foundation e.V., *Pages - Introduction — openHAB*, Dec. 2022. [Online]. Available: https://next.openhab.org/docs/tutorial/pages_intro.html (visited on 01/18/2023).

[27] Thread Group Inc., "Thread 1.1.1 Specification," en, 2017.

[28] *Node Roles and Types*, en. [Online]. Available: https://openthread.io/guides/thread-primer/node-roles-and-types (visited on 01/22/2023).

[29] Connectivity Standards Alliance, “Matter Device Library,” en. [Online]. Available: https://csa-iot.org/wp-content/uploads/2022/10/22-27351-001_Matter-1.0-Device-Library-Specification39.pdf.

[30] M. Adalier, “Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256,” en,

[31] Andrew Blok and Ry Crist, *Matter Smart Home Devices Dominated CES This Year - CNET*, Jan. 2023. [Online]. Available: https://www.cnet.com/home/smart-home/matter-smart-home-devices-dominated-ces-this-year/ (visited on 01/22/2023).

[32] W. Hultström and A. Bjöörn, *Comfort and Security, But at What Cost? : A Study Using a Metric – Based Conjoint Analysis to Estimate the Willingness to Pay for Bundled Smart Home Technology*, eng. 2022. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-314322 (visited on 01/21/2023).

[33] ubisys, *Matter – ubisys Conflux bridge*. [Online]. Available: https://www.ubisys.de/technologie/matter/ (visited on 01/19/2023).