2. Literature Review

2.1 Smart home ecosystems

Smart home ecosystems represent the network on the basis of which communication standards implement data transmission and control of devices (Dasgupta et al., 2019). In such an ecosystem, individual IoT devices are interconnected in a cohesive topology that enables communication between the devices via defined standards. A large number of devices with different functions can be located in a smart home IoT. These include, for example, power and light switches, door locks, roller shutters, sensors, control devices, as well as end devices of everyday life such as household appliances and telecommunications and entertainment devices.

In principle, different communication standards can be used in an ecosystem, but they must be compatible with each other to ensure the interoperability of devices. Due to the respective advantages and disadvantages of the individual communication standards, none of the currently used standards can be identified as a universal application solution of IoT in the smart home area. Several standards are therefore often implemented in parallel in an ecosystem to use the application-related strengths (Tightiz & Yang, 2020).

2.2 Communication standards in the smart home area

To understand the problems of commonly used communication standards, some of the dominant communication standards in the IoT smart home area, Wi-Fi, Bluetooth Low Energy, Thread, Zigbee and MQTT are examined for their strengths and weaknesses.

A distinctive feature of communication standards is the differentiation between wired and wireless standards. While wired standards like Ethernet require a physical transport medium in the form of a cable, wireless standards use radio frequencies to transmit data. In this project, however, only wireless standards are discussed, as these constitute the fundamental innovation of Matter (CSA, 2021). To highlight the problems of the currently used communication standards, the most common wireless standards in the IoT smart home area are considered in the sections 2.2.1 – 2.2.5.

2.2.1 Wi-Fi

One of the most used wireless communication standards is IEEE-802.11, also known as Wi-Fi (IEEE Standards Association, 2021). Through the Wi-Fi Alliance certification process, manufacturers can prove that their devices meet the guidelines of the standard and can therefore communicate with other Wi-Fi enabled devices (Wi-Fi Alliance, 2010). Consumers can thus easily see whether a device is compatible with their network. The Wi-Fi standard describes uniform communication using a wireless local area network (WLAN). WLAN is the umbrella term for Wi-Fi certified devices, so from a technical point of view there are no significant differences (Badman & Parmenter, 2020). As a result, IoT Wi-Fi devices in the smart home area can be easily embedded into the existing WLAN network, making it user-friendly (Danbatta & Varol, 2019).

In the IEEE 802.11 standard, the first two layers of the OSI model, physical layer and data link layer, are defined more precisely (IEEE Standards Association, 2021). Protocols such as IP and TCP/UDP can be used based on the layers of the Wi-Fi standard to define the network and transport layers. Most Wi-Fi networks are built in a star topology in which each device is connected to a central connection node and all communication takes place via this point. Communication as well as authentication in the network takes place via a central access point (AP), which is mainly implemented by a router and connects the network to the Internet (Ding et al., 2018). However, because of the mesh technology, it is also possible to form a network with several APs. This can increase the range as well as the area coverage (Kirichek et al., 2020). Compared to other standards, the Wi-Fi communication standard is primarily characterised by its high data transmission rate of up to 11.2 Gbit/s (Nguyen et al., 2019). On the other hand, this is accompanied by high power consumption of the devices. In summary, the use of Wi-Fi devices is particularly recommended in areas of application that allow a direct connection to the power grid.

Wi-Fi security is achieved through Wi-Fi Protected Access Version 3 (WPA3), although older versions of WPA are no longer considered secure (Alhamry & Elmedany, 2022). WPA3 includes secure authentication in the network, as well as encryption of data traffic (IEEE Standards Association, 2021). However, it should be noted that WPA3 also has security vulnerabilities (Baray & Ojha, 2021). With the help of the Dragonfly handshake, communication is established which supports both elliptic curve cryptography and finite field cryptography (Appel & Guenther, 2020). Thus, WPA3 offers a better security measure than the previous versions, but still has some vulnerabilities that can be exploited if implemented improperly (Vanhoef & Piessens, 2018).

2.2.2 Bluetooth Low Energy

Another communication standard used in the smart home sector is Bluetooth Low Energy (BLE). The standard, designed for short distances, was developed by the Bluetooth Special Interest Group (SIG) (Bluetooth SIG, N.D.). Like Wi-Fi, BLE operates on the 2.4 GHz frequency band and is characterised by lower power consumption, but has lower data transmission rates of up to 2 Mbit/s (Bluetooth SIG, 2023). Figure 1 shows the BLE architecture based on the OSI reference model.

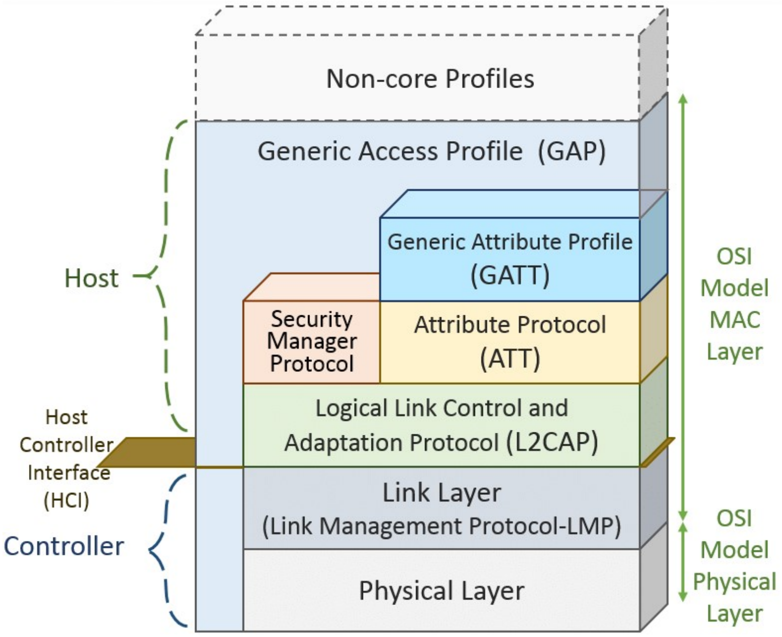
Non-core Profiles
Generic Access Profile (GAP)
Generic Attribute Profile (GATT)
Security Manager Protocol
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Link Layer (Link Management Protocol-LMP)
Physical Layer
Host
Host Controller Interface (HCI)
Controller
OSI Model MAC Layer
OSI Model Physical Layer

Figure 1: BLE protocol stack (Oliveira et al., 2019)

It can be stated that, in contrast to Wi-Fi, the complete BLE protocol stack differs depending on the application (Bluetooth SIG, 2023; Gomez et al., 2012). Another advantage of BLE can be found in the easy implementation of devices in the network. The advertiser opens the connection and regularly sends out broadcast packets, making it visible to connectable devices. The scanner in turn searches for possible connection partners and can initialise the connection setup. A password is not required for the coupling, but there is the possibility that the advertiser must first confirm the incoming connection manually in order to set up a connection so that no unwanted couplings are created.

Once a connection has been established, the sending party is called ‘Active’ and the receiving party is called ‘Standby’. Since Bluetooth 4.1, these roles are no longer static, so that mesh networks are also possible with BLE (Darroudi & Gomez, 2017). With the introduction of Bluetooth 4.2, support for the transmission of IPv6 packets was also developed.

From a security point of view, however, the Bluetooth standard has conceptual vulnerabilities. The authentication and encryption of existing connections is implemented with the Advanced Encryption Standard (AES) algorithm in combination with cipher block changing message authentication code (CCM) mode, which is considered to be a strong encryption method (Mewada et al., 2016). However, the connection establishment is not secure, so that without appropriate precautions in the application layer, all messages can be read until the coupling is completed (Darroudi & Gomez, 2017).

2.2.3 Thread

The Thread communication standard, developed by the Thread Group, was published in 2014 and is thus the newest of the standards examined (Randewich, 2014). Thread was developed to provide a wireless connection between low power devices, using the 2.4 GHz spectrum and is based on IEEE 802.15.4 radio technology (Thread Group, N.D.). Suitable for both small and large networks, the standard communicates via IPv6 (Rzepecki et al., 2018). The comparison of Thread with the OSI model in Figure 2 shows that the physical layer and the data link layer are adopted from the IEEE 802.15.4 standard.

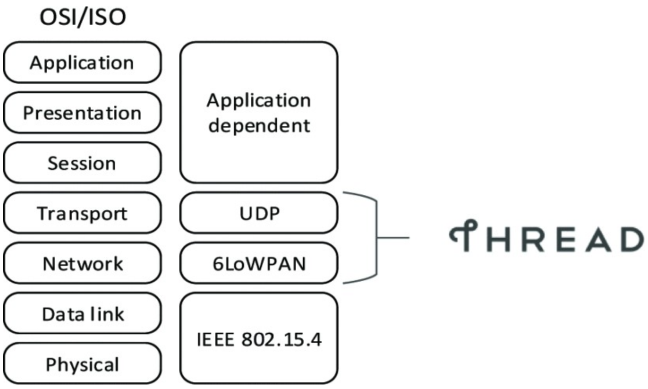

Figure 2: Thread comparison with OSI (Rzepecki & Ryba, 2019)

On the network layer, Thread uses the 6LoWPAN network protocol, which allows the transmission of IPv6 packets over the IEEE 802.15.4 standard and enables the mesh topology (Unwala et al., 2018). An advantage resulting from the application for resource-poor devices is the flexible size of the packet header, which, in contrast to the fixed header sizes in the IPv4 protocol, enables a lower network load. However, this is also necessary because of the low data transfer rate of 250 kbp/s (Samuel, 2016). Thread uses UDP for the transport layer, whereas the layers above it are defined by the application and are therefore not part of the standard.

Border routers are required as gateways to the Thread network to enable Internet capability and the control of Thread devices via end devices that cannot communicate directly via Thread (Unwala et al., 2018). A second border router can be used for improved reliability. Thread routers are solely responsible for communication within a Thread network and can dynamically change routes to maintain reliability in the event of failure, with the centre of the network always being a leader who registers the other routers in the network and manages their responsibilities (Herrero, 2022).

With Thread, the security of the communication is realised with a network-wide key. As with BLE, the AES-CCM method is used for encryption, while the key exchange is based on the Diffie-Hellmann method (Marksteiner et al., 2017; Akestoridis et al., 2022). However, since there is only one key in a network, the compromise of one device is sufficient to be able to decrypt all devices and their communication, which means that insecurely designed IoT devices pose a serious threat to the entire network.

2.2.4 Zigbee

Another common communication standard in the smart home environment is Zigbee, which was specially developed for the requirements of the IoT. Zigbee was developed and standardised by the Zigbee Alliance, now Connectivity Standards Alliance, a global consortium of companies (CSA, N.D.b). The protocol stack of Zigbee is shown in Figure 3.

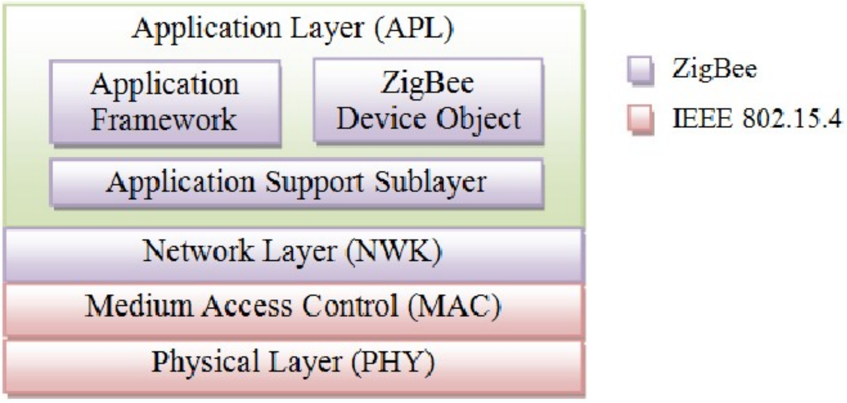

Figure 3: Zigbee protocol stack (Sung et al., 2010)

Like Thread, the standard is based on the IEEE 802.15.4 standard, which specifies the physical and data link layers and is defined by the Zigbee standard from the network layer onwards (Zigbee Alliance, 2016). This enables ZigBee-enabled devices from different manufacturers to be compatible with one another.

Another advantage of Zigbee is its low energy consumption. Zigbee devices can be battery powered and have long battery life making them ideal for IoT applications using batteries (Alobaidy et al., 2020). This is made possible by minimising data transmission. Devices based on the Zigbee standard can spend most of their time in a standby state to extend battery life. For transmission, the standard can communicate on a frequency of 2.4 GHz as well as on sub 1 GHz frequency bands (Zigbee Alliance, 2016).

The ability to self-organise is also an advantage of Zigbee. Zigbee devices can automatically connect to a network and form a mesh network (Adi et al., 2021). This improves the resilience and reliability of the network as there are alternate communication paths in case a device fails or the signal is weak. Furthermore, the simple design based on the IEEE 802.15.4 standard, low hardware requirements and the Zigbee open source model enable comparatively low manufacturing costs (Long & Miao, 2019).

A disadvantage of Zigbee is the limited bandwidth. The standard was mainly developed for low data rate applications, such as sensor data or control information, so the maximum data transmission rate is 250 Kbit/s (CSA, N.D.c). Another disadvantage is the limited range of Zigbee. Although Zigbee devices can achieve greater range over mesh networks, the single range of a Zigbee device is limited compared to other wireless standards such as Wi-Fi or Bluetooth (Adi et al., 2021). Furthermore, Zigbee devices do not support communication with computing devices, since in most cases they do not have a Zigbee module. Therefore, a bridge is required for the smart home with Zigbee, which takes over the distribution of the commands.

With Zigbee, communication is encrypted using the AES-CCM method (Zohourian et al., 2023). However, this is not used on the data link layer as defined in the IEEE 802.15.4 standard, but on the network layer. In this way, routing information can be read by forwarding entities (Khanji et al., 2019). As a result, attackers could use side channel attacks to eavesdrop on the distribution of the keys and thus decrypt the encryption.

2.2.5 MQTT

Message Queuing Telemetry Transport (MQTT) is an open source communications standard specifically designed for transferring messages between devices with limited bandwidth and high latency. It was developed by IBM in 1999 and handed over to the Eclipse Foundation as an open standard in 2010 as part of the MQTT project (Yuan, 2021). MQTT is widely used in the Internet of Things (IoT) to enable efficient and reliable communication between devices and applications. The standard is based on a publish-subscribe model, in which messages are sent from a publisher to one or more subscribers (International Business Machines Corporation & Eurotech, 2015). This model allows for loose coupling between the devices and applications involved. MQTT uses a lightweight protocol over TCP/IP that incurs little overhead and minimises the resource load on the devices involved.

A major advantage of MQTT is its efficiency and scalability. As MQTT is a lightweight standard, it requires less bandwidth and storage compared to other communication protocols (Soni & Makwana, 2017). In addition, MQTT supports a variety of topologies, with multiple publishers and subscribers. This enables scalable and flexible communication between many devices and applications. Another advantage of MQTT is its reliability. It supports message receipt with acknowledgment to ensure messages were successfully transmitted (Atmoko et al., 2017). This reliability is particularly important in applications where critical information is transmitted.

MQTT also offers high flexibility and interoperability. It is platform independent and can be implemented on different operating systems and devices (Bender et al., 2021). There are also a large number of MQTT brokers who act as intermediaries between publishers and subscribers. These brokers can run on different systems and enable communication between devices from different manufacturers. This enables seamless integration and collaboration between devices.

Despite these advantages, MQTT also has some disadvantages. A disadvantage is the limited support for complex data structures. MQTT mainly supports the exchange of simple messages transmitted as strings or binary data (Soni & Makwana, 2017). MQTT is less suitable for applications that require complex data structures or extensive metadata. Furthermore, MQTT does not have any standardised security functions (Chen et al., 2020). Security must be implemented through additional mechanisms such as Transport Layer Security (TLS) or Virtual Private Networks (VPNs) to ensure secure communication. This can mean additional implementation effort and increase complexity.

2.3 Challenges of interoperability between communication standards

Inadequate compatibility can mean that certain functions of the devices cannot be used. This problem is referred to as a lack of interoperability between smart home devices and manufacturers (Noura et al., 2019). ISO (2015) defines interoperability as, "*capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units*".

A central cause of interoperability problems results from the large number of device types, which have different functions and thus address different data structures (El Jaouhari et al., 2019). In many communication standards, profiles are predefined at the application level, which classify the most important functions of a device type (Valtchev et al., 2002). This has the advantage that not every manufacturer has to implement every function of a device individually and can focus on innovations. However, in terms of interoperability, this property of the standards poses a challenge. In order for all messages in a network to be translated from one protocol to another, gateways must know all the application profiles used (Phan & Kim, 2020). With an increasing number of manufacturers and IoT devices, it is no longer practical for gateway manufacturers to implement this large number of application profiles. If a gateway is not able to translate the data of a device on the application level, it follows that not all functions of the device can be used properly.

To solve the interoperability problems, one approach could be a universal communication standard (Hazra, et al., 2021). This relieves the gateways of a manageable number of application profiles. However, a comparison of existing communication standards in IoT shows that each standard has its own advantages and disadvantages, so that the corresponding standards are currently used depending on the area of application and operating system used (Samuel, 2016). Another possible solution is the development of a gateway that is able to dynamically add application profiles from the manufacturer's servers to its own database (Aloi et al., 2016; Phan & Kim, 2020). It must be assumed here that the application profiles are made freely available by the manufacturers. Taking into account the large number of manufacturers and IoT devices, this approach represents a major organisational and political effort.

The initiative to develop a uniform IoT framework was initiated by the Open Interconnectivity Foundation (OCF) in 2016 (OFC, N.D.) OFC aims to develop a publicly accessible framework to counteract fragmentation in the IoT landscape. The framework sets guidelines for interoperability between different standards in a network. In order to ensure interoperability, it is recommended to use IPv6 at the network layer level, which applies to each of the considered communication standards (OCF, 2022). However, the largest and leading manufacturers have also taken on the challenge of interoperability problems and have been developing the new communication standard Matter in cooperation under the leadership of the Connectivity Standard Alliance (CSA) since 2020.

2.4 Threats of IoT in smart home

IoT devices have limiting factors in terms of size and power consumption due to their areas of application. This limitation of performance capacity is accompanied by technical limitations of possible implementations of security mechanisms (Gupta, 2019). However, the economical manufacture of IoT devices also contributes to the vulnerability of IoT systems (Chantzis et al., 2021). Many companies place an emphasis on device cost effectiveness, which in turn makes device security an undesirable expense. This also means that buyers are usually not sufficiently informed about the secure configuration of the devices (Emami-Naeini et al., 2019). It should also be considered that IoT systems can often be used for several decades without having to be replaced (Chantzis et al., 2021). Devices without Internet access in particular are therefore subject to the increasing risk that these devices are not secured against newly discovered vulnerabilities.

Numerous attacks on IoT networks and smart home ecosystems have been discovered and published in recent years (Dorobantu & Halunga, 2020). It is possible to classify these attacks into known patterns. One type of attack is signal jamming, where the goal is to disrupt the transmission between two devices, thereby affecting the availability of the system (Alhammadi & Zaboon, 2022). This is typically achieved by sending interfering signals, which means that the devices can no longer receive relevant messages from the radio traffic.

Another common type of attack is the replay attack, in which an attacker tries to read messages between two devices and then sends them to the original recipient. It is not necessary for the attacker to crack the encryption mechanisms used in order to manipulate the behaviour of the target device (Marksteiner et al., 2017). While battery-powered IoT devices can lead to a targeted increase in power consumption and thus massively decrease battery lifetime, such attacks can lead to serious health risks in the context of medical IoT devices (Butt et al., 2019).

In setting tampering attacks, attackers try to change the configuration of the target device (Chantzis et al., 2021). For example, this can result in malicious server requests being accepted or all incoming requests being blocked. In addition, IoT devices are often vulnerable to hardware integrity attacks. These are attacks that involve physical access to the device hardware, such as malicious code injection through an unprotected USB port (Abomhara & Køien 2015).

Since IoT systems usually include a large number of devices, attackers can try to imitate legitimate devices via node cloning attacks (Mogbil et al., 2020). In this way, an attacker could imitate the control unit in a network and thereby gain access to the entire network. All attacks in which communication between devices in a network is intercepted can be summarised under the term security and privacy breaches (Chantizis et al., 2021). The attackers monitor network communication and, if necessary, try to circumvent the encryption of the messages in order to read out relevant information. In addition, the risk of human error always remains. This includes, for example, social engineering or phishing attacks, where an attacker can gain control of the system (Ali & Award, 2018).

The use of IoT standards and frameworks, such as those provided by Matter, offer manufacturers support, as they already implement many security mechanisms and thus simplify and accelerate development. However, this support can also lead to a false perception of security. There is an assumption that a most widely used framework or communication standard already has sufficient security measures when in reality there may be fundamental security problems (Gupta, 2019).

References

Abomhara, M. & Køien, G. M. (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility* 4: 65-88. Available from: https://journals.riverpublishers.com/index.php/JCSANDM/article/view/6087 [Accessed 09 May 2023].

Adi, P. D. P., Sihombing, V., Siregar, V. M. M., Yanris, G. J., Sianturi, F. A., Purba, W., Tamb, S. P., Simatupang, J., Arifuddin, R. & Prasetya, D. A. (2021) 'A performance evaluation of ZigBee mesh communication on the Internet of Things (IoT)', *3rd East Indonesia Conference on Computer and Information Technology.* Surabaya, Indoneisa, 09-11 April. IEEE. 7-13. Available from: https://ieeexplore.ieee.org/abstract/document/9431875 [Accessed 17 June 2023].

Akestoridis, D. G., Sekar, V. & Tague, P. (2022) 'On the security of Thread networks: Experimentation with OpenThread-enabled devices', *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks.* San Antonio, Texas, 16-19 May. New York: Association for Computing Machinery. 233-244. Available from: https://dl.acm.org/doi/abs/10.1145/3507657.3528544 [Accessed 21 April 2023].

Alhammadi, N. A. M. & Zaboon, K. H. (2022) A Review of IoT Applications, Attacks and Its Recent Defense Methods. *Journal of Global Scientific Research* 7(3): 2128-2134. Available from: https://www.gsjpublications.com/jgsr15920059.pdf [Accessed 25 March 2023].

Alhamry, M. & Elmedany, W. (2022) 'Exploring Wi-Fi WPA2 KRACK vulnerability: A review paper', *International Conference on Data Analytics for Business and Industry*. Sakhir, Bahrain, 25-26 October. IEEE. 766-772. Available from: https://ieeexplore.ieee.org/abstract/document/10041548 [Accessed 02 September 2023].

Ali, B. & Awad, A. I. (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* 18(3): 817. Available from: https://www.mdpi.com/1424-8220/18/3/817 [Accessed 09 May 2023].

Alobaidy, H. A., Mandeep, J. S., Nordin, R. & Abdullah, N. F. (2020) A review on ZigBee based WSNs: concepts, infrastructure, applications, and challenges. *International Journal of Electronical Engineering & Telecommunications* 9(3): 189-198. Available from: http://www.ijeetc.com/uploadfile/2020/0414/20200414052006525.pdf [Accessed 18 June 2023].

Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W. & Savaglio, C. (2016) 'A mobile multi-technology gateway to enable IoT interoperability', *IEEE first international conference on internet-of-things design and implementation.* Berlin, Germany, 04-08 April. IEEE. 259-264. Available from: https://ieeexplore.ieee.org/abstract/document/7471371 [Accessed 24 April 2023].
Appel, M. & Guenther, I. S. (2020) *WPA 3-Improvements over WPA 2 or broken again?*. Munich, Char of Network Architectures and Services, Department of Informatics. Available from: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2020-11-1/NET-2020-11-1_02.pdf [Accessed 02 May 2023].

Atmoko, R. A., Riantini, R. & Hasin, M. K. (2017) IoT real time data acquisition using MQTT protocol. *Journal of Physics: Conference Series* 853(1): 012003. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/853/1/012003/pdf [Accessed 19 June 2023].

Badman, L. & Parmenter, T. (2020) What is the difference between WLAN and Wi-Fi?. *TechTarget*. Available from: https://www.techtarget.com/searchnetworking/answer/Wireless-vs-Wi-Fi-What-is-the-difference-between-Wi-Fi-and-WLAN [Accessed 19 April 2023].

Baray, E. & Ojha, N. K. (2021) 'WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique', *5th International Conference on Computing Methodologies and Communication.* Erode, India, 08-10 April. IEEE. 23-30. Available from: https://ieeexplore.ieee.org/abstract/document/9418230 [Accessed 19 July 2023].

Bender, M., Kirdan, E., Pahl, M. O. & Carle, G. (2021) ‚Open-source mqtt evaluation', *IEEE 18th Annual Consumer Communications & Networking Conference.* Las Vegas, USA, 09-12 January. IEEE. 1-4. Available from: https://ieeexplore.ieee.org/abstract/document/9369499 [Accessed 19 June 2023].

Bluetooth SIG (2023) The Bluetooth Low Energy Primer. Available from: https://www.bluetooth.com/wp-content/uploads/2022/05/The-Bluetooth-LE-Primer-V1.1.0.pdf?__hstc=44473531.2faf1062bd3216c20d1374676e323ce9.1681978224809.1681978224809.1681978224809.1&__hssc=44473531.6.1681978224809&__hsfp=278970564&hsCtaTracking=8e3cb9ce-2e7b-471a-b5cc-2343a4915b6a%7C090f705a-f0df-4f4b-8a54-c8f97c73eb69 [Accessed 20 April 2023].

Bluetooth SIG (N.D.) Bluetooth Wireless Technology. Available from: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/ [Accessed 20 April 2023].

Butt, S. A., Diaz-Martinez, J. L., Jamal, T., Ali, A., De-La-Hoz-Franco, E. & Shoaib, M. (2019) 'IoT smart health security threats', *19th International conference on computational* *science and its applications.* St. Petersburg Russia, 01-04 July. IEEE. 26-31. Available from: https://ieeexplore.ieee.org/abstract/document/8853599 [Accessed 08 May 2023].

Chantzis, F., Stais, I., Calderon, P., Deirmentzoglou, E. & Woods, B. (2021) *Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things*. No Starch Press. Available from: https://learning.oreilly.com/library/view/practical-iot-hacking/9781098128876/c02.xhtml#h1-500907c02-0002 [Accessed 23 March 2023].

Chen, F., Huo, Y., Zhu, J. & Fan, D. (2020) ‚A review on the study on MQTT security challenge', *IEEE International Conference on Smart Cloud.* Washington, USA, 06-08 November. IEEE. 128-133. Available from: https://ieeexplore.ieee.org/abstract/document/9265962 [Accessed 19 June 2023].

CSA (2021) The Future of IoT is Now: Project Connected Home over IP. Available from: https://www.youtube.com/watch?v=Dqy6ASRgWmI [Accessed 05 April 2023].

CSA (N.D.a) The Foundation for Connected Thing. Available from: https://csa-iot.org/all-solutions/matter/ [Accessed 16 March 2023].

CSA (N.D.b) zigbee – The Full-Stack Solution for All Smart Devices. Available from: https://csa-iot.org/all-solutions/zigbee/ [Accessed 19 June 2023].

CSA (N.D.c) Zigbee FAQ. Available from: https://csa-iot.org/all-solutions/zigbee/zigbee-faq/ [Accessed 19 June 2023].

Danbatta, S. J. & Varol, A. (2019) 'Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation', *7th International Symposium on Digital Forensics and Security.* Barcelos, Portugal, 10-12 June. IEEE. 1-5. Available from: https://ieeexplore.ieee.org/abstract/document/8757472 [Accessed 19 April 2023].

Darroudi, S. M. & Gomez, C. (2017) Bluetooth low energy mesh networks: A survey. *Sensors* 17(7): 1467. Available from: https://www.mdpi.com/1424-8220/17/7/1467 [Accessed 20 April 2023].

Dasgupta, A., Gill, A. Q. & Hussain F. (2019) 'Privacy of IoT-Enabled Smart Home Systems', in: Ismail, Y. (eds) *Internet of Things (IoT) for Automated and Smart Applications.* IntechOpen. 9-24. Available from: https://mts.intechopen.com/storage/books/7602/authors_book/authors_book.pdf [Accessed 30 March 2023].

Ding, J., Li, T. R. & Chen, X. L. (2018) The application of Wifi technology in smart home. *Journal of Physics: Conference Series* 1061(1): 012010. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/1061/1/012010/meta [Accessed 19 April 2023].

Dorobantu, O. G. & Halunga, S. (2020) 'Security threats in IoT', *International Symposium on Electronics and Telecommunications.* Timisoara, Romania, 05-06 June. IEEE. 1-4. Available from: https://ieeexplore.ieee.org/abstract/document/9301127 [Accessed 08 May 2023].

El Jaouhari, S., Jose Palacios-Garcia, E., Anvari-Moghaddam, A. & Bouabdallah, A. (2019) Integrated management of energy, wellbeing and health in the next generation of smart homes. *Sensors* 19(3): 481. Available from: https://www.mdpi.com/1424-8220/19/3/481 [Accessed 24 April 2023].

Emami-Naeini, P., Dixon, H., Agarwal, Y. & Cranor, L. F. (2019) 'Exploring how privacy and security factor into IoT device purchase behavior', *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems.* Glasgow, Scotland, 04-09 May. New York, Association for Computing Machinery. 1-12. Available from: https://dl.acm.org/doi/abs/10.1145/3290605.3300764 [Accessed 08 May 2023].

Gomez, C., Oller, J. & Paradells, J. (2012) Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors* 12(9): 11734-11753. Available from: https://www.mdpi.com/1424-8220/12/9/11734 [Accessed 20 April 2023].

Gupta, A. (2019) *The IoT Hacker's Handbook*. Berkeley, CA: Apress. Available from: https://learning.oreilly.com/library/view/the-iot-hackers/9781484243008/ [Accessed 24 March 2023].

Hazra, A., Adhikari, M., Amgoth, T. & Srirama, S. N. (2021) A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. *ACM Computing Surveys* 55(1): 1-35. Available from: https://dl.acm.org/doi/abs/10.1145/3485130 [Accessed 24 April 2023].

Herrero, R. (2022) *Fundamentals of IoT Communication Technologies*. Cham: Springer. Available from: https://link.springer.com/content/pdf/10.1007/978-3-030-70080-5.pdf [Accessed 21 April 2023].

IEEE Standards Association (2021) 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. Available from: https://standards.ieee.org/ieee/802.11/7028/ [Accessed 13 April 2023].

International Business Machines Corporation & Eurotech (2015) MQTT V3.1 Protocol Specification. Available from: https://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html [Accessed 19 June 2023].

ISO (2015) ISO/IEC 2382:2015. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v2:en [Accessed 07 April 2023].

Khanji, S., Iqbal, F. & Hung, P. (2019) 'ZigBee security vulnerabilities: Exploration and evaluating', *10th international conference on information and communication systems.* Irbid, Jordan, 11-13 June. IEEE. 52-57. Available from: https://ieeexplore.ieee.org/abstract/document/8809115 [Accessed 17 June 2023].

Kirichek, R., Vishnevsky, V. & Koucheryavy, A. (2020) ‘Analytic model of a mesh topology based on LoRa technology’, *22nd International Conference on Advanced Communication Technology.* Phoenix Park, South Korea, 16-19 February. IEEE. 251-255. Available from: https://ieeexplore.ieee.org/abstract/document/9061519 [Accessed 19 April 2023].

Long, S. & Miao, F. (2019) ‘Research on ZigBee wireless communication technology and its application’, *IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference.* Chengdu, China, 20-22 December. IEEE. 1830-1834. Available from: https://ieeexplore.ieee.org/abstract/document/8997928 [Accessed 31 July 2023].

Marksteiner, S., Jimenez, V. J. E., Valiant, H. & Zeiner, H. (2017) ‘An overview of wireless IoT protocol security in the smart home domain’, *Internet of Things Business Models, Users, and Networks.* Copenhagen, Denmark, 23-24 November. IEEE. 1-8. Available from: https://ieeexplore.ieee.org/abstract/document/8260940 [Accessed 21 April 2023].

Mewada, S., Sharma, P. & Gautam, S. S. (2016) ‘Exploration of efficient symmetric AES algorithm’, *Symposium on Colossal Data Analysis and Networking.* Indore, India, 18-19 March. IEEE. 1-5. Available from: https://ieeexplore.ieee.org/abstract/document/7570921 [Accessed 20 April 2023].

Mogbil, R., Asqah, M. & Khediri, S. (2020) ‘Iot: Security challenges and issues of smart homes/cities’, *International Conference on Computing and Information Technology.* Univeristy of Tabuk, Sudi Arabia. 9-10 September. IEEE. 1-6. Available from: https://ieeexplore.ieee.org/abstract/document/9213827 [Accessed 09 May 2023].

Nguyen, K., Golam Kibria, M., Ishizu, K. & Kojima, F. (2019) Performance evaluation of IEEE 802.11 ad in evolving Wi-Fi networks. Available from: https://www.hindawi.com/journals/wcmc/2019/4089365/ [Accessed 31 May 2023].

Noura, M., Atiquzzaman, M. & Gaedke, M. (2019) Interoperability in internet of things: Taxonomies and open challenges. *Mobile networks and applications 24*: 796-809. Available from: https://link.springer.com/article/10.1007/s11036-018-1089-9 [Accessed 24 April 2023].

OCF (2022) OCF Core Specification. Available from: https://openconnectivity.org/specs/OCF_Core_Specification.pdf [Accessed 24 April 2023].

OCF (N.D.) OCF SOLVING THE IOT STANDARDS GAP. Available from: https://openconnectivity.org/ [Accessed 24 April 2023].

Oliveira, L., Rodrigues, J. J., Kozlov, S. A., Rabêlo, R. A. & Albuquerque, V. H. C. D. (2019) MAC layer protocols for Internet of Things: A survey. *Future Internet* 11(1): 1-42. Available from: https://www.mdpi.com/1999-5903/11/1/16 [Accessed 31 May 2023].

Phan, L. A. & Kim, T. (2020) Breaking down the compatibility problem in smart homes: A dynamically updatable gateway platform. *Sensors* 20(10): 2783. Available from: https://www.mdpi.com/1424-8220/20/10/2783 [Accessed 18 April 2023].

Randewich, N. (July 15, 2014) Google's Nest launches network technology for connected home. *Reuters*. Available from: https://www.reuters.com/article/us-google-nest-idUSKBN0FK0JX20140715 [Accessed 09 May 2023].

Rzepecki, W. & Ryba, P. (2019) 'Iotsp: Thread mesh vs other widely used wireless protocols–comparison and use cases study', *7th International Conference on Future Internet of Things and Cloud.* Istanbul, Turkey, 26-28 August. IEEE. 291-295. Available from: https://ieeexplore.ieee.org/abstract/document/8972835 [Accessed 09 May 2023].

Rzepecki, W., Iwanecki, Ł. & Ryba, P. (2018) 'IEEE 802.15. 4 thread mesh network–data transmission in harsh environment', *6th International Conference on Future Internet of Things and Cloud Workshops*. Barcelona, Spain, 06-08 August. IEEE. 42-47. Available from: https://ieeexplore.ieee.org/abstract/document/8488173 [Accessed 31 July 2023].

Samuel, S. S. I. (2016) 'A review of connectivity challenges in IoT-smart home', *3rd MEC International conference on big data and smart city.* Muscat, Oman, 15-16 March. IEEE. 1-4. Available from: https://ieeexplore.ieee.org/abstract/document/7460395 [Accessed 19 April 2023].

Soni, D. & Makwana, A. (2017) 'A survey on mqtt: a protocol of internet of things (iot)', *International conference on telecommunication, power analysis and computing techniques.* Chennai, India, 12 April. Research Gate. 173-177. Available from: https://www.researchgate.net/profile/Dipa-Soni/publication/316018571_A_SURVEY_ON_MQTT_A_PROTOCOL_OF_INTERNET_OF_THINGSIOT/links/58edafd4aca2724f0a26e0bf/A-SURVEY-ON-MQTT-A-PROTOCOL-OF-INTERNET-OF-THINGSIOT.pdf [Accessed 19 June 2023].

Sung, T. W., Wu, T. T., Yang, C. S. & Huang, Y. M. (2010) Reliable data broadcast for zigbee wireless sensor networks. *International journal on smart sensing and intelligent systems* 3(3): 504-520. Available from: https://sciendo.com/article/10.21307/ijssis-2017-405 [Accessed 31 July 2023].

Thread Group (N.D.) What is Thread?. Available from: https://www.threadgroup.org/What-is-Thread/Overview [Accessed 21 April 2023].

Tightiz, L. & Yang, H. (2020) A comprehensive review on IoT protocols' features in smart grid communication. *Energies* 13(11): 1-24. Available from: https://www.mdpi.com/1996-1073/13/11/2762 [Accessed 18 April 2023].

Unwala, I., Taqvi, Z. & Lu, J. (2018) 'Thread: An iot protocol', *IEEE Green Technologies Conference.* Austin, Texas, 07 June. IEEE. 161-167. Available from: https://ieeexplore.ieee.org/abstract/document/8373620 [Accessed 21 April 2023].

Valtchev, D. & Frankov, I. (2002) Service gateway architecture for a smart home. *IEEE Communications Magazine* 40(4): 126-132. Available from: https://ieeexplore.ieee.org/abstract/document/995862 [Accessed 24 April 2023].

Vanhoef, M. & Piessens, F. (2018) ‘Release the Kraken: new KRACKs in the 802.11 Standard’, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* Toronto, Canada, 15-19 October. New York, Association for Computing Machinery. 299-314. Available from: https://dl.acm.org/doi/abs/10.1145/3243734.3243807 [Accessed 19 April 2023].

Wi-Fi Alliance (2010) Wi-Fi certified Wi-Fi Direct. Available from: https://www.wi-fi.org/system/files/wp_Wi-Fi_Direct_20101025_Industry.pdf [Accessed 19 April 2023].

Yuan, M. (2021) Getting to know MQTT. Available from: https://developer.ibm.com/articles/iot-mqtt-why-good-for-iot/ [Accessed 19 June 2023].

Zigbee Alliance (2016) Base Device Behavior Specification Version 1.0. Available from: https://csa-iot.org/wp-content/uploads/2022/01/docs-13-0402-13-00zi-Base-Device-Behavior-Specification.pdf [Accessed 18 June 2023].

Zohourian, A., Dadkhah, S., Neto, E. C. P., Mahdikhani, H., Danso, P. K., Molyneaux, H. & Ghorbani, A. A. (2023) IoT Zigbee device security: A comprehensive review. *Internet of Things*, 22: 100791. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2542660523001142 [Accessed 18 June 2023].