ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

Evaluation of Security Features of the Smart Home Protocols ZigBee, Z-Wave, Thread, BLE, and EnOcean with Focus on the Role of the End User

An Updated Literature Review Applying the PRISMA 2020 Guide

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Anna Maria Riedl
Is181824

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: Dipl.-Ing. Oliver Eigner, BSc

Tulln an der
Donau,
24.05.2023

(Unterschrift Autor/Autorin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Tulln an der
Donau,
24.05.2023

(Unterschrift Autor/Autorin)

Table of Contents

List of Figures

List of Tables

Zusammenfassung

Für das Internet der Dinge gibt es ein breites Spektrum an Sicherheitslücken. Diese Zahl steigt von Jahr zu Jahr, da immer mehr Geräte auf den Markt kommen und immer mehr Anwendungsfälle für das IoT entdeckt werden. Viele Angriffe auf solche Netzwerke haben sich als verheerend erwiesen, nicht nur für das menschliche Leben, sondern auch aus wirtschaftlicher Sicht. Cybersicherheitsvorfälle können einen finanziellen Schaden in Milliardenhöhe verursachen; der Rufschaden, den ein betroffenes Unternehmen erleidet, ist unermesslich. Entwickler*innen und Hersteller*innen sind sich dieser Situation bewusst und haben kontinuierlich an Gegenmaßnahmen gearbeitet, um die Netzwerk- und Individualsicherheit zu erhöhen. Die in ZigBee, Z-Wave, Thread, BLE und EnOcean implementierten Sicherheitsmerkmale werden in dieser Arbeit diskutiert. Diese Arbeit ist eine aktualisierte Literaturübersicht zu den Sicherheitsmerkmalen der einzelnen Protokollstapel der zuvor genannten Protokolle. Die Forschung wird auch herausfinden, wie die Endnutzer*innen in den Sicherheitsprozess eines Netzwerks eingebunden sind. Ziel dieser Arbeit ist es auch, zu prüfen, ob seit den früheren Literaturübersichten zu diesem Thema neue Sicherheitsmerkmale hinzugekommen sind. Um der Arbeit und ihren Ergebnissen Qualität und Struktur zu verleihen, besteht der Hauptbeitrag dieser Arbeit in der Umsetzung des PRISMA 2020-Rahmens für Meta-Analysen. Dieser Rahmen wurde, soweit erkennbar, bei Literaturübersichten im IT-Sektor noch nicht verwendet. PRISMA 2020 wird von Forschern in der Medizin, Pharmazie, Linguistik und anderen wissenschaftlichen Bereichen verwendet, um ihre Arbeiten in bestmöglicher Qualität durchzuführen. Die Ergebnisse der Literaturrecherche werden in Form einer Tabelle dargestellt und die Erkenntnisse anschließend kurz diskutiert. Es hat sich herausgestellt, das zum Protokoll EnOcean kaum verwertbare Literatur existiert, während an den Protokollen ZigBee, Z-Wave, Thread und BLE immer wieder Erweiterungen zur Verbesserung der Cybersicherheit und Privacy vorgenommen werden. Weiterhin stehen die End-Nutzer*innen als teilnehmende Parteien an passiver Stelle, wodurch sich eine potenzielle Forschungslücke ergibt: Die Rolle der End-Nutzer*innen in einen aktiveren Part zu setzen und zu erforschen, welche Sicherheitsfeatures und -maßnahmen durch sie ergänzt werden können.

Abstract

For the Internet of Things, a wide range of security vulnerabilities exists. This number is only increasing with each year, as more and more devices enter the market and more use cases for IoT are discovered. Many attacks on such networks have proven to be devastating not only for human life but also from an economic point of view. Cyber security incidents can cause billions of dollars of financial damage; the damage of reputation an affected organisation suffers is immeasurable. Developers and manufactures are alert to this situation and have continuously worked on countermeasures to increase network and individual security. The security features implemented in ZigBee, Z-Wave, Thread, BLE, and EnOcean are discussed in this work. This work is an updated literature review to the security features of each protocol stack of the previously named protocols. The research will also discover how the end users are involved in the security process of a network. It is also the goal of this thesis to check whether there have been new security features added since the previous literature reviews on this topic. To add quality and structure to the work and its result, the main contribution of this work is the implementation of the PRISMA 2020 framework for meta-analyses. This framework has not been used in literature reviews in the IT sector as far as was discernible. PRISMA 2020 is used by researchers in the medical, pharmaceutical, linguistic, and other scientific sectors to conduct their works and deliver the best possible quality. The results of the literature research are presented as a table and the findings then discussed shortly. It has been found that little literature exists on the EnOcean protocol, while ZigBee, Z-Wave, Thread, and BLE protocols continue to be enhancedand researched to improve their respective cybersecurity and privacy features. Further, end-users are passive participating parties in a network when it comes to the security features of it, being protected by features already implemented by software developers and manufacturers, creating a potential research gap: Putting the role of end-user in a more active part and exploring what security features and measures can be added by them.

Introduction

Smart Home and the Internet of Things (or short IoT) have been two terms that have become highly relevant in the past two decades. When people hear either of these terms, they associate a fully automated house and devices that can carry out all their tasks on their own without the human user needing to interfere with them. Both Smart Home and IoT have been used synonymously although each term describes a different area of usage. Smart Home comprises the home a person or family with small devices that can connect to the Internet. These devices have the purpose of automating basic functions of daily life (e.g., light bulbs, radiators, dish washers, washing machines, security cameras, thermometers, air conditioners etc.). These devices are small, and resource constrained as they usually have only a single purpose to fulfil as well as being able to connect to the Internet. Users set up a centralized unit for data accumulation where all the data the smart devices in their households have gathered are being sent, stored, and evaluated for future decision making. The devices in a Smart Home can be managed and addressed either via an app, through a voice communication assistant or directly on the devices (e.g., the user turns on the light by themselves). Whereas the Internet of Things contains all the small devices that are scattered over the Internet, constantly collecting data, and sending to a processing unit where it is stored and evaluated. Contrary to a Smart Home, where the border is where the premises of the housing ends, the boundaries of the Internet of Things are not fixated. It can be said though that Smart Homes are part of the Internet of things. However, they are not the Internet of Things. IoT describes an enormous cluster and areas of operation where the so called “Things” are deployed and form mostly mesh networks with varying topologies. Among these areas of operation is Smart Home. Due to the limited hardware resources the devices in a Smart Home are prone to have security vulnerabilities. Malicious users on the Internet may exploit these vulnerabilities when they discover them and cause great financial and, in some cases, even physical harm. Therefore, proper protection is indispensable[1].
This thesis focuses on the analysis of currently existing literature on the topic of security features in common protocols that are implemented in smart home devices. The aim is to point out relevant work on the topic of smart home protocols and their security features, with a special focus on the role of the end user. The thesis points out how the user is involved in the implementation of security in their smart home setup.

The Chapter “Basic Information“ covers basic information about IoT and Smart Home. The fields of operation for IoT are listed and explained. The protocols that are examined in this thesis are explained in the chapter as well.

The Chapter “Cybersecurity in Smart Home Setups“ deals with the topic of cybersecurity in Smart Home setups. Challenges in the environment of Smart Home are elaborated on. Attacks in the IoT environment are discussed and a short explanation on the weaknesses of the Smart Home protocols analysed in this thesis is given.

The Chapter “Security Features“ is focused on the various security features of ZigBee, Z-Wave, Thread, BLE, and EnOcean. The chapters are structured into the fields of application for the protocol, followed by the security features implemented into the protocol stacks.

The Chapter “Approach, Methods, and Analysis“ explains the method chosen for the analysis, the searching criteria, the keyword definition for the search strings, the search strings, and lastly, the process of screening the results. The chosen method, PRISMA 2020 is elaborated on. The platforms for the search are listed and the syntax of the search strings required for each search platform is explained. The tool used for collecting and screening the search results is discussed shortly.

The Chapter “Results of Literature Analysis“ presents the results of the literature research in a table depicting author(s), title, purpose, type of source, year, protocols, major themes, attacks/threats mentioned, countermeasures proposed, and user interaction.

Chapter “Discussion“ offers a discussion on each of the items contained in the table of chapter “Results of Literature Analysis“.

The Chapter “Concluding Words and Future Research” as the final chapter of this thesis gives a short summary of what was done, how the results were achieved, what results have been found and which questions have been answered. Research gaps are described as well. Furthermore, the chapter contains an outlook on possible future research and a short conclusion.

Basic Information

In this chapter general information on smart home and smart grids is provided to give an idea of the field in question. The advancements of technology in smart home and smart grid projects are outlined in later sections of this chapter. The rising importance of smart home setups inspired several well-known companies to participate in the market. Among the most well-known are Apple, Microsoft, Samsung, Phillips, and Google. The devices currently available in the general product range are mentioned among the list of devices presented later in this chapter. The list contains a selection of devices that may be utilized in a smart home setup such as dish washers, washing machines, lamps, light bulbs, air conditioners, voice assistants, and many more.

Definition of Internet of Things/Smart Home

In this subsection, the use cases for IoT are listed and discussed shortly to create as complete an overview as possible. Among the various use cases is smart home, which is the use case in focus of this thesis.
The first use case according to Swamy et al. [2] concerns “Infrastructure Monitoring”. This use case deals with Pipeline monitoring in the oil and gas industry to detect leakages and failures along the way to the refinery. It is also utilized in monitoring the civil structure, or more accurately, to look for cracks, damages, leaks, stress, displacement, and other irregularities in bridges, railways, buildings, monuments, and roads. Infrastructure Monitoring also assists the military and may be used for surveillance reasons. Lastly, Infrastructure Monitoring is helpful for monitoring aircraft health with the objective of increasing efficiency in field operation, and to detect possible hazards.
The next use case defined by Swamy et al. [2], named “Smart Agriculture” concerns, as the name suggests, everything concerning crops, watering plants, and livestock. In Smart Agriculture, however, the term “Precision Farming” is used when it comes to monitoring the environmental conditions as well as the soil so that farmers can tend to their crops’ needs, thus generating a better harvest. Then, there is “Crop Health Monitoring”, especially meant for detecting whether crops are suffering from dehydration, fungi infection or other bacteria that could harm the plant. To keep track of a farmer’s livestock, there is “Livestock Monitoring”, meant to keep a close eye on animals’ grazing behaviour, digestion, and on their overall health condition as well as probable injuries on the animals. For free running livestock, it is important to the farmer to track them across the pasture and see if there has been a trespassing beyond pasture borders. Finally, for crops that grow in greenhouses, there is the sub-use case of “Green House Monitoring” which makes it possible for a farmer to grow different crops with different needs in the same greenhouse. This is made possible by creating the best conditions for each plant according to data the sensors in the growing zones pick up.
The third use case, “Smart Home”, also defined by Swamy et al. [2], is the centre topic of this work’s research and a few ways to utilize it are explained as follows. An alternate term for Smart Home and used often instead of Smart Home is Home Automation. Home Automation describes a set up where

the residents of a housing unit install the means to centrally, remotely and without too much user interaction, control their appliances. Such appliances may be heating, air conditioning, fans, window shutters, kitchen appliances (e.g., dish washer, toaster, coffee machine, fridge, oven, …), windows and doors, security cameras, lighting utilities, power outlets, and TVs. An entire branch of research and development (which is not part of this thesis due to time resources) is dedicated to Indoor Air Quality Management to prevent increased levels of pollutants, and consequently, open the windows of that certain room or the housing unit. This cuts into the area of Smart Healthcare, which is discussed later in this section, as it assists, e.g., asthmatic residents to keep their symptoms to a minimum and therefor enhance quality of life within their own four walls. As an extension, Elderly People Monitoring provides a means to help detecting emergencies, accidents, or alarming decreases in overall health conditions of elderly residents. A Smart Home may extend beyond a room and concern the Gardening of a residential building. Especially, when residents are away for longer periods of time, or absent during the day, the health of their plants and crops are constantly monitored for hydration levels and nutrition requirements. Pest control may be included in Smart Gardening. As mentioned previously, Surveillance of the housing unit is part of product lines concerned with home security (not to be confused with cyber security as this focuses on security of assets more than physical security of residents) and is meant to secure the home against intruders, trespassers, and burglars.

The fourth use case, “Smart Health” [2], may be utilized in private homes as well as in medical environments, such as hospitals and retirement homes. It helps with diagnosing patients early on through sensors, wearables, and implantable sensors. This technology enables doctors to monitor the health condition of their patients remotely and in real-time. Private individuals have been moving in the field of Smart Health through the fitness sector. This sector utilizes the sensors implemented in wearables to measure the level of physical activity in a person’s life. People make use of this technology to monitor their movement throughout the day as well as the intensity and their overall health condition. Blood pressure, blood Oxygen, pulse, sleep, menstruation and burned calories are among the variables that can be measured. The data gathered by the wearables may be collected on a smart phone and even used to create a medical profile, which can be shown to doctors for a better insight on the person’s overall condition. The possibility to measure these things on one’s own also act as a potential motivator to get in more movement which in turn improves personal health. In Smart Health there is also “Emergency Care” which helps in cases of accidents and occurrence of natural disasters to find a nearby hospital or call emergency services, should the victim(s) be rendered incapable of doing so by themselves.

The fifth use case, called “Smart Retail” [2], enables tracking of items or shipments via sensors. This helps to prevent theft or track stolen items. On a broader scale, Smart Retail, gives the technology to perform automated checkout processes and provide recommender Systems.

The sixth use case, “Smart Power and Water Grids” [2], is designed to fully automate the generation, measurement, and distribution of electric power and water to citizens in residential areas. In a Smart Power grid power losses during the distribution phase are monitored. Sensors are also collecting data on load balancing and metering, which is then processed to adjust load balancing scales or distribution to households. This leads to the next task of managing and distributing the resources to citizens. Energy consumption of households and industrial areas is measured through the collected data on energy and water usage and electrical energy.

The seventh use case Swamy et al. [2] have defined is called “Factory Automation and Industry 4.0”. As the name suggests this use case for IoT is utilized in the industrial sector. One example is “Plant Safety”, an application where the overall condition of the manufacturing plant and the worker’s safety is monitored. Possible hazards are detected and analysed. Incidents like fire, overexert, caught in machine, and slip & fall accidents are inspected. Another example for the effective utilization of Industry 4.0 is the monitoring of products in the product development life. Bottle necks are detected and reduced, and the entire production process is then optimized for future use. In supply chain management, product information is shared in real-time to improve the supply chain operation. Quality control ensures that the end products is free from faults by analysing the products at critical points in production and alerting when substandard quality is found.
The eighth use case, “Environmental Monitoring” [2], is used to detect and monitor, e.g., forest fires. Environmental Monitoring may also be used for finding water reservoirs, manage water distribution, and for water sanitization. The outdoor air quality in cities can be measured to reduce the risk of sicknesses due to pollution in the population. It is also possible to implement mechanisms to detect natural disasters and provide accurate safety measures for the citizens in the area.
The second last use case, “Smart Cities” [2], combines the use cases Smart Energy, Smart Homes, Smart Industry, and Environmental Monitoring, and encompasses electric grids and water grids as well as transport infrastructure. Transport infrastructure describes everything from walkways, streets, highways, railways, and subterranean transport routes. In Smart Cities “E-Governance” can be implemented, which describes the process of providing government services to the citizens via information technology. The communication ways can be government-to-citizen (G2C), government-to-employees (G2E), government-to-business (G2B), government-to-government (G2G) as well as covering back-office processes within the entire government framework. Smart Communities are created and work to the community’s needs for water supply, energy, waste disposal, water sanitization, and leakage identification. This happens on a smaller scale than the previously mentioned use case Smart Energy and Water. The data collected and applied for decision making in Smart Communities is used for energy sector though. Public areas are under surveillance to reduce crime rate and provide visual data where officers cannot normally detect incidents.
The final use case for IoT concerns “Intelligent Transportation” [2]. Within Intelligent Transportation there are several smaller areas to make use of the technology. One such area is the “Traveller’s Information System (TIS) which is designed for travellers who need information on the location, traffic conditions and regulations, possible routes, emergency services, safety, and warnings. This information is provided to travellers who can access it anytime anywhere. Then there is Traffic Flow and Control which is meant for areas with high traffic and population density. Cameras are placed at every crossroads or points of interests and shared the collected data among the travellers. The Freight Management System (FMS) gathers information on freight at sea, in air, or on land in real-time. The data is then used to optimize freight carriage operations. Finally, there is Vehicle-to-Vehicle communication (V2V) in which tracking is a process where two vehicles communicate and share information about surrounding infrastructure and other vehicles in the vicinity with each other.

The Internet of Things in general comprises many ubiquitous devices, all connected and constantly collecting data and exchanging it with each other. Each device is uniquely identified [3] and accessible through the Internet. IoT is realized in a growing number of applications such as

healthcare monitoring, smart agriculture, smart city, smart grid, utilities, animal farming, home security and emergency, smart water, industrial control, transportation, environmental monitoring, and smart home. The latter is part of this thesis' focus.
Naglic et al. [4] speak of smart home as the representation of an ideal partner in solving energy inefficiencies occurring in households. This claim is founded on the centrally managed topology of smart home setups. They promote the idea to establish a connection between smart home and smart grid which would benefit the distributors in managing the power grid efficiently.
According to Naglic et al. a "smart home" describes a modern way of living that stands in contrast to the conventional living environment. In any given smart home setup, a variety of process atomization is offered that would require manual work in a non-smart-home environment.

Examples for automation according to Naglic et al. include:

- Lighting
- Temperature and ventilation control
- Kitchen equipment
- Home appliances
- Computer and consumer electronics
- Home energy management
- Security
- Window and door operation

What Naglic et al. define as smart home, however, requires no user-interaction once the setup is finished. The devices pick up data from sensors and, according to that data, act, e.g., shut the windows, turn on the heat, start air conditioning based on outside temperatures and so on.
The main feature of smart home appliances is their connectivity and interoperability. Smart devices (the devices utilized in a smart home setup) are controlled and managed centrally either through home energy controller (automated) or via voice command (user must interact). These voice commands are processed by a voice assistant unit, e.g., Alexa, Bixby, Google Assistant, Cortana, or Siri.
The integration of the smart devices is possible if they are compatible with these communication protocols or protocol stacks [4] [3]:

- ZigBee
- Z-Wave
- KNX
- LoRaWan
- SigFox
- WirelessHart
- OS41
- BLE
- IEEE 802.15.4
- WiFi

- NFC
- IPSec
- Thread
- EnOcean
- 6LoWPAN
- RPL
- CoAP
- MQTT
- XMPP
- AMQP

Among these examples Naglic et al. [4] list Ethernet as a means for communication between smart home devices though devices that utilize wireless protocols are more likely to be used by consumers. Wireless devices offer a better usability as well as easy integration. They are thus more prevalent.
The devices in a smart home may be connected to the internet using ISP technologies like xDSL, FFTH or LTE/5G. When a user wants to utilize commands from outside his home network they can do so via VPN (Virtual Private Network), which makes communication over the Internet more secure for their data.
The connection is utilized via an ISP gateway like a router and from that point communication is taking place over protocols like ZigBee, Z-Wave and many more.
Some of the protocols mentioned in the previous sentence are part of this thesis' topic and a detailed description of their features are found in chapter “Security Features“.

In [2] the authors list the pillars of IoT as follows:

- Sensing & Automation
- Identification
- Communication
- Computation
- Services
- Management
- Security

The wireless connection has the advantage of increased simplicity, high availability, high bandwidth rate and lower latency.
The security features of wireless protocols are described in chapter “Security Features“.

In [5], there is a short note on the term “Internet of Things” being introduced for the first time in 1999 in a presentation at P&G by Kevin Ashton. Ashton described IoT as a necessity to implement since available data is increasing exponentially and therefore cannot be captured, managed, or supervised by humans alone any longer.
At its core, the idea of IoT is meant to connect people with things regardless of place, time, who one wants to connect with and with any possible service.
Overall, IoT is also to be understood as a network consisting of more networks (see smart grid, smart cities, smart factories, smart vehicles, etc).

There are several sensor technologies which may be considered the backbone of the IoT. One of these technologies is Near Field Communication (NFC), among others like Radio Frequency Identification (RFID), Wi-Fi, ZigBee and Bluetooth. The latter two are discussed in this thesis, albeit the traditional Bluetooth protocol will not be part of this work. However, the Bluetooth protocol, BLE, which was specifically developed for IoT, is part of the discussion and literature analysis.
A note on NFC and RFID: These technologies may also be utilized for device registration with an IoT Cloud Server [6]. This approach requires an application interface on an NFC capable mobile device. The application is opened by the user, who then places the device they wish to register within proximity to the smartphone and thus initializes the registration process. This is one of the ways to connect things with a user and each other as presented by [6].

General Architecture of IoT

Ahmadi et al. [5] define several possible architectures that can be deployed in the IoT. In this subsection these architectures will be listed shortly.

Three Layers

In a Three Layers architecture there are, as the name suggests, three layers, each of which has a group of tasks to perform so the purpose of the network is met. The first layer is the Perception Layer, also known as “Sensor Layer”. This layer is responsible for interaction with physical devices through technologies like RFID. Its main purpose is to integrate things or other objects into IoT and prepare them for interacting with higher layers.
The next layer is the Network Layer or “Transmission Layer”. This layer handles the information provided to it by the perception layer. It also watches the data transmission routes to the IoT hubs. In this layer the communication protocols are implemented (Bluetooth, LTE, 3G, …).
The third and final layer is the Application Layer. This layer receives data provided by the network layer and uses this data to create services which are provided to the user.

Five Layers

This concept has the three layers previously presented but provides two additional layers on top of these[5].
One of the additional layers is the Middleware Layer. This layer exists between the network and the application layer, and it is responsible for handling the scalability, coordination, availability of services, Quality of Service (QoS) as well as reliability.
The other additional layer is the Business Layer. This layer is placed on top of the application layer, and it aggregates all information from an IoT network. This collected information is then used for forming conclusion and finding trends, which is necessary to suggest solutions based on forecasting.

SoA Architecture

This architecture follows the same basic functions as the Three-Layer architecture, only it adds a service layer in between network and application layer.

The service layer consists then of service discover, service composition, service management and service interfaces [5].

Workgroups for Smarthome

Among the Workgroups that are responsible for the development of the smart home protocols discussed in this work are Matter, ZigBee Alliance [3], Z-Wave Alliance [7], and the Thread Group.

Furthermore, the groups IEEE and IETF play into the picture of these protocols. Each of the Groups and institutions are explained shortly in this subsection.

Matter

In December 2019, Amazon, Apple, Google, and the ZigBee Alliance announced the forming of Matter, which is an IP-based standard opting for maximum connectivity and compatibility in the smart home sector. The initial name for this project was “Connected Home over IP” or in short “CHIP”. The project was rebranded as “Matter” in May 2021 [8]. Among the available smart home protocols, Thread has been the only IEEE802.15.4-based networking protocol selected for the Matter standard.

Thread Group

This group has developed Thread, a smart home protocol meant to be application-agnostic and enabling IPv6-based low-power mesh networking.

ZigBee Alliance/Connectivity Standards Alliance (CSA)

Originally, the ZigBee Alliance was created to develop a set of standards for IoT to tackle the plethora of protocols flooding the market. The mission was and is to this day, to simplify, harmonize, and build global standards for IoT. The main concern is to make IoT ethical, sustainable, and secure.

Z-Wave Alliance

Z-Wave is a proprietary protocol owned by Sigma Designs, while the Z-Wave Alliance promotes it [9]. The protocol has been originally designed by the Danish company Zensys in 2001, and it is meant specifically for the field of application in home automation [10].

IEEE

IEEE or Institute of Electrical and Electronics Engineers is the world’s largest organization dedicated to advancing technology for the benefit of humanity. IEEE is known for its highly cited publications, conferences, technology standards, and educational activities [11].

As of 2022 the organization counts more than 427,000 members across the globe in more than 190 countries. There are more than 145,000 student members. In addition, IEEE, leads in the development of international standards, many of which contributed to the current landscape of technology and global connection.

Smart Home Protocols

In this section, the protocols that are in focus of this thesis are elaborated on. The protocols mentioned in this section are all part of the literature survey, the results of which are discussed in chapter “Results of Literature Analysis“.

ZigBee Protocol

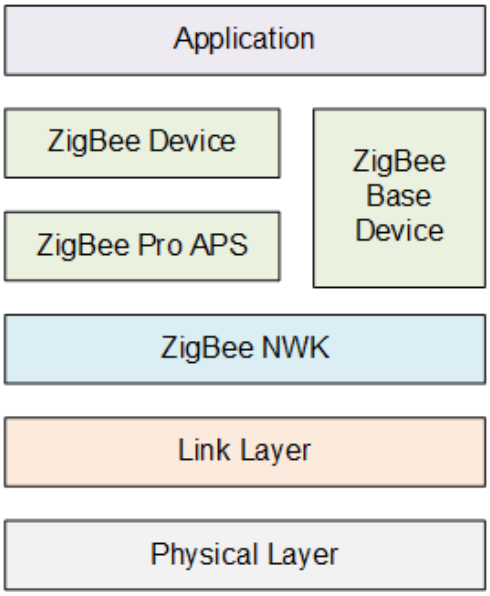


Figure 1: Abstract depiction of the ZigBee protocol stack [12]

The ZigBee protocol is based on the IEEE 802.15.4 specification. The Physical (PHY) and MAC Layer have been redefined according to this specification to make low power, low cost, and low complexity possible for ZigBee [13]. Some of the features of ZigBee [13] include low power consumption which is ideal for sensor networks and this is supported by the low cost factor of ZigBee. In addition, the network capacity of ZigBee expands up to 65,536 nodes in one network. Despite the low power consumption and low-cost feature, ZigBee provides a reliable overall network with numerous security features included. Another feature provided by ZigBee is its flexible working frequency band.
ZigBee is a protocol developed by the ZigBee Alliance and its protocol stack is based on top of IEEE 802.15.4. IEEE 802.15.4 provides the physical and MAC layers which is the reason for ZigBee being compatible all hardware that is built adhering to IEEE 802.15.4 [3]. The protocol stack further supports star, tree, and mesh routing topologies.
There are three main components within a ZigBee network: the Controller (ZC), the router (ZR), and the end device (ZED) [12]. ZC and ZR may never go into sleep mode, therefore they require a constant power supply as the ZED are not allowed to let other devices join the network and must communicate exclusively through their ZR. Upon creation of the network the ZC assigns a network ID. In a ZigBee network there are four ways to exchange network parameters upon the authorization of devices:

1. Association
2. Rejoin
3. Rejoin via orphaning
4. Out-of-Band

Z-Wave Protocol

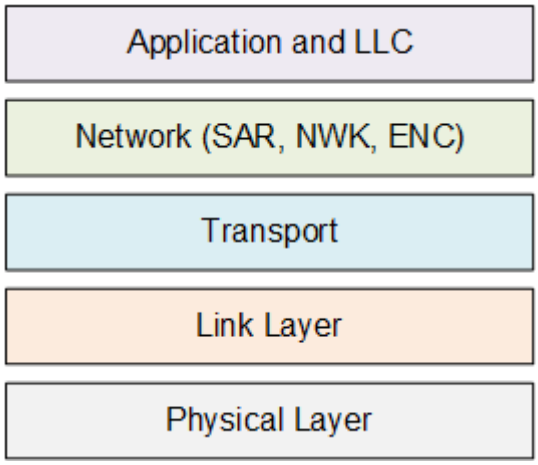


Figure 2: Abstract depiction of the Z-Wave protocol stack [12]

Z-Wave is a proprietary protocol owned by Sigma Designs, while the Z-Wave Alliance promotes it [9]. The protocol has been originally designed by the Danish company Zensys in 2001, and it is meant specifically for the field of application in home automation [10].
Z-Wave has been found vulnerable to MITM attacks, traffic analysis and spoofing due to the protocol's inherent requirement to be able to operate with older devices that may not support the security features mentioned in "Z-Wave" [7]. When a device newly joins a network, a preconfigured key, encrypted with a fixed value is shared. This key may be extracted easily by utilizing traffic analysis.
Due to the trust model of Z-Wave, impersonation attacks may be executed without detection.
It also up to each manufacturer to decide whether or not they will ship their devices with AES 128-bit encryption mechanism included or omit this feature. [7] mention that less than 50% of shipped devices support encryption.
Z-Wave is a good protocol for networks where the maximum range between nodes exceeds 30 meters. This distance can be covered by the protocol due to the low frequency it is set at. It is also the preferable choice to, e.g., ZigBee since the frequency rate is unaffected by interferences that happen on the 2.4GHz band [7]. The operating frequency varies for Z-Wave. In Europe and partially in Asia the rate is 868.4MHz while it is set to 908.4MHz in the USA [5]. Currently 130 countries have the transmission frequencies for Z-Wave available and this number is expected to further expanse [14].
Z-Wave has a master/slave architecture, meaning there is one master (the home gateway) in a network controlling the slave nodes. The network master needs to have all the data about the network in advance, including the information of all devices that will join the network [9].

In [10] there is a slightly different version of the protocol stack defined by the authors; this version consists of four layers instead of five. The authors do not mention a dedicated Link Layer in their model. Instead, the protocol stack defined by Kim et al. [10] mentions a Physical Layer, Transport Layer, Routing Layer, and Application. They are the first and only authors found within the research parameters of this thesis to assign an entire layer to the task of routing and forego the Link Layer in their description.

Physical Layer

The main task of this layer is to transfer data between the nodes, using either one of three supported data rates: 9.6 kbps (R1), 40 kbps (R2), and 100 kbps (R3) [15].

MAC Layer

Z-Wave utilizes CSMA/CA on the MAC layer to get access to the medium which, in this case and contrary to ZigBee, uses IEEE 802.11 RTS/CTS. The MAC layer knows three types of MAC frames it can handle: single-cast, multi-cast, and acknowledgment [15].

Adaptive Layers (NWK, SAR, ENC)

The third layer is split into three divisions, all specialized on dealing with different tasks. NWK handles all the networking. SAR is responsible for Segmentation and Reassembly of datagrams. ENC handles the encryption of the split datagrams before they are sent on their way. Z-Wave works with the AES or Rijndael 128-bit keys length.

LLC Layer and Application Layer

handled. One such function is the Binary Switch to either turn a device of or on, request a device status or rrespond to a request. These three actions are issued using either one of three commands available to the Binary Switch: *Get*, *Set*, and *Report* [14].

In 2012 Z-Wave was added to the International Telecommunication Union (ITU-T) as an open standard G.9959 [14] [10].

In Z-Wave, messages are exchanged a synchronously over the RF medium in the form of MAC Protocol Data Unit (MPDU) frames [16].

Thread

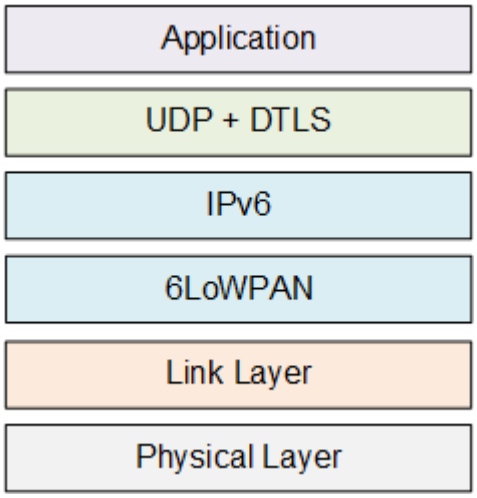


Figure 3: Abstract depiction of Thread protocol stack [12]

Thread uses the IEEE 802.15.4 MAC implementation. However, there were some modifications, e.g. the CSMA/CA is required by the specification, just as active and energy detect scan, exchanging MAC data ACK, data request frames, exchanging beacon frames, and MAC frame security. Not permitted are: periodic beacons, guaranteed time slots, generating or interpreting, PAN coordinator frame [5].

BLE

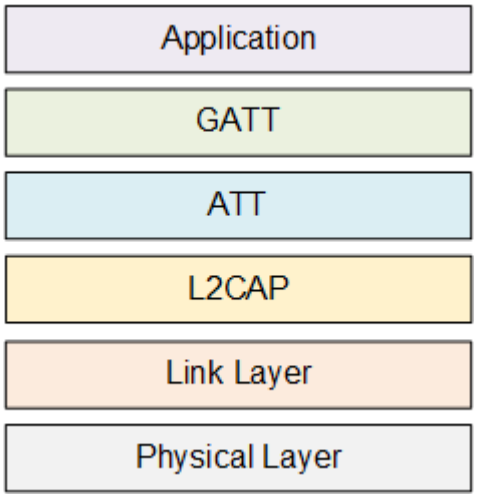


Figure 4: Abstract depiction of the BLE protocol stack [12]

BLE has been developed for devices that communicate wireless and transfer data in this manner. An alternate name for BLE is Bluetooth 4.0 [17]. The main driver behind the specification is the same group that is also responsible for defining and maintaining the Bluetooth standard: the Bluetooth SIG Group. This group has defined services for BLE. The protocol is currently deployed in billions of

devices across the globe. BLE differs from the classic Bluetooth protocol in its simplified protocol stack which was designed to target low-energy, low-cost devices [18].
BLE utilizes 40 communication channels on the 2.4 GHz frequency, of which 3 are used for advertising packets, while the remaining 37 channels are for data exchange only [12].
Through the ATT layer data can be accessed. Attributes are stored on the central server and BLE clients can access them.
According to [19] a BLE device can assume one of two roles: central or peripheral. Peripheral devices are known to have lower capacities and send out advertisements which are picked up by the central device. Central devices need to scan continually for advertisements as they are responsible for initiating the connection between the peripheral device and themselves. Devices can only be discovered through advertisement. Advertisements are prevented from colliding with each other by a mechanism which determines a random wait period for the device between 0 and 10ms before the next advertisement is sent [19]. Once a connection has been established, the peripheral device starts frequency hopping and monitors the timeout interval which is exchanged between the central and the peripheral device on connection establishment. If no answer is received from the central device, the connection is dropped. After the peripheral is connected it must not send advertisement beacons out again. It can however send non-connectable advertising messages. This approach, however, gives away information to any listening party in the vicinity as the message contains the device's name, type, and address [19].

In [20] another version of the BLE protocol stack is listed. This version is much more detailed and displays the Bluetooth 4.0 stack, explaining the features of each layer in detail.

BLE has a 6-byte address known as BD_ADDR, which is similar in design to the one implemented in the classic Bluetooth protocol. This address can be either static or private, the former is generated once and never changes afterward, the latter changes periodically [20].

Besides the BD_ADDR the BLE protocol also has a preamble which is used to synchronize the receiver at the start of the frame and which responds to a series of alternating bits (0x55) [21].
Also, on the PHY layer of BLE, there is a field called Protocol Data Unit (PDU) which is made up of a link-layer header as well as the data that needs to be transmitted.
Finally, the PHY layer defines a Cycle Redundancy Check (CRC), a field 3 bytes in length with the purpose of integrity checking.
Data is prefixed with the link-layer header, then encapsulated into the PDU field, and finished up with the CRC sum. The preamble and BD_ADDR are added to the frame before it is sent.

EnOcean

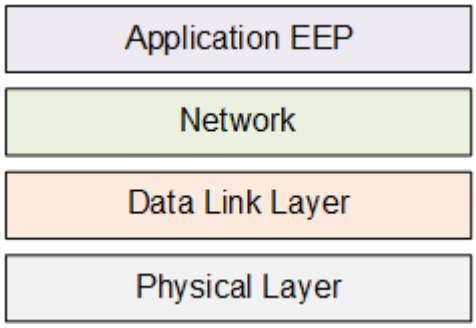


Figure 5: Abstract depiction of the EnOcean protocol stack [12]

The features of EnOcean are simultaneously the security features and are as such presented in chapter “Security Features”.

Cybersecurity in Smart Home Setups

In this section a short overview on the importance of cybersecurity in smart home setups is given. The idea of smart homes has been around since the mid-seventies of the 20th century where the first smart home platform was introduced.
The devices in a smart home will be connected to the Internet and transmit data to a centralized management centre. As mentioned in chapter “Definition of Internet of Things/Smart Home“ the smart home may be controlled via app on a mobile device.
This connection to the Internet may allow attackers to conduct exploits to gather data from the smart home devices in a household. This is supported by the increasing number of device connections which offers a greater attack surface.

Challenges in the IoT Environment

There are challenges concerning the privacy, identity management and addressing security vulnerabilities.
The traditional triad according to which security threats can be categorized had to be expanded due to insufficiencies in the IoT environment [5].

In IoT environments, devices must fulfil security challenges even though the devices in such a network operate with limited resources, meaning, they possess small memory, have little performance, low energy radios and often limited operating time due to battery size [22].

Security challenges in an IoT environment are connected to the implementation of strong authentication, authorization, privacy, confidentiality, ensuring data integrity, establishment of a trust-based relationship between devices, and physical security.

The CIA triad principles to be achieved in an IoT network have been integrated into the IAS-octave which has been cultivated to encompass more focus points than the initial triad, and as such, cover a wider cyber security area in a non-traditional setting [5].

The IAS-Octave consists of the following cyber security areas:

- Confidentiality
- Integrity
- Availability
- Access Control
- Comprehensive Perception
- Reliable Transmission
- Intelligent Processing
- Global Laws

To illustrate the attack landscape an IoT environment presents [5] have provided an overview of attacks based on the aforementioned three-layer architecture. The table illustrates how each layer is prone to a different type of attack (see Figure 6). This presentation of attacks is used as a reference in this thesis to create a keyword list later, based on which the literature research and analysis, the centre focus of this thesis is conducted.

In [6] the attack surface of an IoT cloud-centric environment is categorized into three main groups: software, memory and storage, and communication. Within the context of these three main groups there are several more categorizations, as illustrated below:

Memory & Storage	Software	Communication
USB	Firmware	RFID
RAM	OS	NFC
HDD	Drivers	Bluetooth
SD	Device Configuration	BLE
SSD	Applications	

Table 1: The three attack surfaces for IoT devices in a cloud-centric IoT framework [6]

The authors of [6] discuss attacks on communication channels shortly, among the attacks eavesdropping, replay, modification, and MITM. Of the three attacks, two may be carried out at close range as well as long range. MITM requires proximity, thus only a close-range attack is possible in this setting.

Perception Layer		Network Layer		Application Layer	
Type of attack	Effects	Type of attack	Effects	Type of attack	Effects
Node Capture Attack	Adversary can capture and control the node	Denial of Service (DoS) attack	Can consume all the available resources in IoT by attacking network protocols or bombarding the IoT network with massive traffic	Phishing attack	Adversary can obtain confidential data of users such as identification and passwords
Malicious Code Injection Attack	Inserts malicious code into memory of the node	Spoofing Attack	Adversary gains full access to the IoT system		
False Data Injection Attack	Adversary can inject false data in place of normal data	Sinkhole attacks	A compromised device or node claims exceptional capabilities of power, computation	Malicious Scripts	Represent the scripts that are added, modified, deleted to software with the purpose of harming systems in IoT
Replay Attacks or Freshness Attacks	Adversary can use malicious node or device to transmit to destination host with legitimate identification information	Wormhole Attacks	Launched by two cooperative malicious devices or nodes in IoT		
Cryptanalysis Attacks and Side Channel Attacks	Use the obtained cipher text or plaintext to infer the encryption key	Man-in-the-middle attack	A malicious device controlled by adversary can be virtually located between two communicating devices in IoT	Malicious Virus/worm	Adversary can infect the IoT applications with malicious self-propagation attacks like worms, Trojan horse
Eavesdropping and Interference	Wireless links can be eavesdropped by non-authorized users	Routing information Attack	Focus on the routing protocols in IoT systems		
Sleep Deprivation Attacks	Breaks the programmed sleep routines and keeps devices or nodes awake all the time	Sybil Attacks	Sybil device can claim several legitimate identities and impersonate them in IoT systems	Cryptographic weakness	Possible to decrypt encrypted data caused by weak encryption
		Unauthorized Access	RFID tags can be accessed, and the information stored in tags can be obtained, modified, and deleted by the adversary		

Figure 6: A presentation of attacks categorized into the layers of a three-layer architecture as it is employed in IoT [5]

Choudhuri et al. [23] group threats in the IoT environment into six categories which are depicted shortly in Table 2.

Attack category	**Attacks**
Communications	Packet injection
Device Master infiltration	Compromise device master, steal personal data, compromise confidentiality and integrity of said data
Perception layer	Packet capture and relay, information tracking, tampering, hijacking, DoS, rogue packet forwarding, compromise gateways

Attack category	Attacks
Physical layer	Jamming, tampering
Network layer	DoS, eavesdropping, illegal data access
Application layer	Tampering, eavesdropping, causing data breaches

Table 2: Categories of threats faced in the IoT environment [23]

Attacks in the IoT Environment

In 2021 the MITRE organization did a research on the 25 most dangerous software weaknesses. Many of these may be present in smart home applications [24].
The number of existing and predicted smart home devices in addition to existing weaknesses leaves opportunity for attackers to exploit these weaknesses. Such exploits have been increasing in the past five years. One of the bigger attacks on wireless devices have included the Mirai Botnet in 2016.

The Mirai Botnet was a means to commence DDoS (Distributed Denial-of-Service) attacks to bring down websites and services including Twitter, Reddit, and Netflix. These services were unusable for several hours. However, any kind of website and infrastructure may be infected and taken down. This is particularly worrisome when it comes to unavailable health care systems, power grids or public infrastructure. The bot used for this type of attack primarily spread by infecting other IoT devices like webcams, DVRs (Data Video Recorders) and routers. Once a device was infected it spread to other IoT devices by carrying out dictionary attacks to get administrative credentials. After infecting a device, the bot waited for a command from the botmaster to attack a target server. The source code for the bot has been published and re-used since 2016, resulting in whole botnets (some of them consisted of up to 400,000 devices) that could be rented by attackers.
The Mirai attack has shown the potential of resource constrained devices to be used for nefarious purposes. Since this famous attack, developers of protocols for IoT setups have implemented security features into their devices and specifications. These features are the focus of this thesis.

In IoT, much like in classical IT networks the CIA principles as well as AAA-Principles are highly recommended to adhere to achieve a proper security level.
To cover these areas as efficiently as possible each device in a network should provide at the minimum authentication mechanisms, authorization to access resources, encrypted connections for key exchange and data transfer, integrity checks of transmitted data, and intrusion detection [5].
The recommended approach by Ahmadi et al. [5] to achieve these features is to combine firewall concepts with encrypted connections (VPN), intrusion detection and prevention as well as deep packet inspection.
this approach is applicable to secure highly critical infrastructures like power grids.

The attacks listed in the following subsections “Eavesdropping” to “Replay Attack” are attacks that are applicable on all IoT protocols in this thesis. Attacks that have been designed to specifically address vulnerabilities of the respective protocol are explained in the chapters dedicated to said protocols.

Eavesdropping

When carrying out an eavesdropping attack, the attacker can choose between active or passive attacks. Eavesdropping is one of the easier attacks since it requires proximity only, not a direct connection to software. One device must be compromised by the attacker either directly or through

viruses and malware. The device can then be left alone and any data that has been captured can be collected by the attacker. Alternatively, the attacker can trigger the device to send the collected data to a predefined collection point [25] [26] [27].

Denial of Service (DoS)

In a DoS attack, the victim's network is either flooded with traffic until services shut down or purposefully crashed by sending dedicated commands to the end devices [28] [25]. Legitimate users and other devices are thus deprived of the service they need to access. Typical flooding attacks include SYN flooding, ICMP flooding, and buffer overflow attacks. When aiming to crash a system, a vulnerability is exploited by the attacker. A derivation from DoS is DDoS, where a target is attacked from several locations at once, not just from one location. This approach makes detection of the attack's origin difficult and therefore, shutting the attack down becomes a greater challenge too.

Node Compromise

Attackers choose a node via discovery, then infiltrate it either by directly accessing it or taking it over through Malware, Trojans, Worms, or Viruses [25].

Wormhole Attack

Wormhole attacks are network layer attacks using advanced nodes that can establish communication channels over a long range. In a wormhole attack scenario, one malicious node forwards collected data to another node on the far end of the network through a tunnel. Using this method enables an attacker to trick the nodes into believing they are in proximity to other nodes when in reality, the target node on the other end of the tunnel is far away [29] [25].
Wormhole attacks can be separated into three categories:

1. **Open Wormhole**: Other nodes in the network that are not used for transferring data are ignored. All data packets are sent from the source to a wormhole that tunnels them to the other wormhole which transmits them to the destination.
2. **Half-open Wormhole**: All data packets are sent from the source to the wormhole and then directly transferred to the destination.
3. **Closed Wormhole**: Data packets are transferred directly from the source to the destination without hops in between.

Sinkhole Attack

In a sinkhole attack scenario, an attacker either compromises a node or introduces a node to the network. The node then proceeds to advertise itself to its neighbors as the shortest path to the base station, thus routing all traffic over itself. The neighboring nodes then gravitate towards the malicious node, including the nearest neighbors to the original base [30] [25].

Physical Attack

This form of attack includes everything that compromises the physical security of a node, e.g. tampering, freezing, burning, smashing, flashing, etc. Attacks on physical security often result in a permanent loss of data on the device, including the device itself [25]. Another way to compromise a node physically is through jamming its signals and inducing a DoS through the RFID chip of the device [31]. Furthermore, an attacker can inject a fake node into a network which then proceeds to carry out other attacks such as passive eavesdropping. Devices may also be prevented to go into sleep mode when they are not actively participating in the network. Attackers force interrupt the SLEEP signal of a node and keep it awake. This attack consecutively leads to battery exhaustion in very small devices and ultimately causes the device to shut down.

Key Extraction

Nodes are compromised and then the process of key generation is infiltrated as well. During the initial key generation, either the generating device or the receiving device may be spied on. From the device's NVRAM the network and communication keys can then be extracted [25].

Key Leakage

Network traffic is intercepted early on and the keys that are shared across the network extracted from the data transmission [25]. The difference to key extraction in this method is that keys are stolen while they are in transit while key extraction steals keys that are at rest on the devices.

MITM

For a successful MITM attack the first step is to intercept traffic in the victim's network through a chosen spoofing attack (e.g., IP spoofing, ARP spoofing or DNS spoofing). Next step is traffic decryption without the user's or network master's notice. This can be done either by HTTPS spoofing (forging certificates and sending them to the victim), SSL BEAST (capturing cookies through malicious scripts), SSL hijacking (passing forged authentication keys to application and device during TCP handshake), or SSL stripping (downgrading HTTPS connection by intercepting the TLS authentication) [25] [32].

Spoofing

Spoofing includes everything that is connected to create a façade that is trustworthy to the victim with the ulterior motive to gain access to confidential connections and data. This data is then intercepted, sniffed, stolen, compromised, or rendered unusable by the attacker [33] [25].

Sniffing

All packets that are passed in a network are being monitored by an attacker and sensitive data is being stolen by using that method [25]. Intruders generate fake traffic and pretend to be legit participants of a network [33].

Replay Attack

In a replay attack, the attacker captures traffic, impersonates the origin, and resends the package to the destination. The receiver gets the same message twice with differentiating origins [34] [25].

Zigbee has no way of detecting whether one of its applications or protocol layers has been compromised due to the implementation of an implicit trust model.

The devices in a ZigBee network are prone to jamming attacks because of the low power communication technique [7].

List of attacks that ZigBee devices are prone to [35]:

- rogue acknowledgement
- packet injection
- replay
- physical attack
- side channel
- network discovery
- same-nonce
- sniffing
- frame trashing
- greedy behavior attack
- battery exhaustion
- end-device sabotage
- PAN-ID conflict
- guaranteed time-slots attack
- CSMA/CA exploit
- Jamming

Protection against these attacks is provided by implementation of the following measures [36]:

- Protected memory of the device to prevent tampering
- Heightened attention on default TC links as these are public and have the same level of protection as unencrypted key transport
- Distribute master keys only via OOB channels
- The network keys should undergo a periodic rotation to avoid key leakage

ZigBee Threats and Attacks

Carnain et al. [25] have presented a dedicated threat model for one protocol used in smart home applications and environments to identify and address threats to the network. The threat model has been developed especially for ZigBee (see Figure 7). This graphic is used to structure the findings of the literature review into four main categories, as seen in the graphic: layer specific, method specific, target specific, and member specific. In short, the security features on the layer specific aspect will concern everything that fights off attacks on the protocol stack's layers. The model applies to Zigbee as defined by Carnain et al., however, the categorization of security features in this manner covers the other protocols examined in this thesis as well.

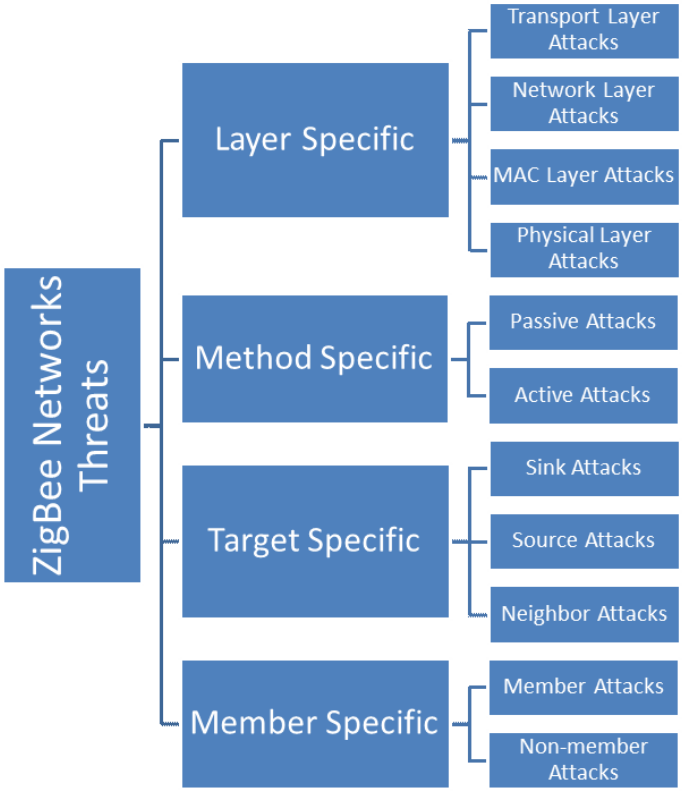


Figure 7: A threat model devised to address known network attacks within a ZigBee network as seen in [25]

Furthermore, the possible attacks on a ZigBee network itself are separated into five categories [25]:

- Eavesdropping
- Denial of Service (DoS)
- Node Compromise
- Sinkhole and Wormhole attacks
- Physical attacks

Z-Wave

Z-Wave was designed by Sigma Designs, Inc. and is meant for remote control applications in residential environments [3]. Z-Wave is proprietary and not open to the public, meaning only the manufacturers have access to the specification and the software development kit. Z-Wave covers all layers in the protocol stack from the physical layer to the application layer. Devices that use Z-Wave have a range of up to 30 meters. On the physical layer, these devices use the Industrial, Scientific, Medical frequency band (ISM) [3]. The frequency rate depends on the continent the network operates on: In Europe the rate is 868.42 MHz while in the US it is 908.42 MHz. The reason this specific frequency was implemented into the protocol was that the devices may need to operate in environment that are prone to interferences due to WiFi channels. By setting the frequency to the rates already mentioned, this interference is bypassed [3].
Each Z-Wave network needs one controller which can support up to 232 active nodes. The controller has a unique Home ID necessary for network identification. Once the manufacturer has configured the Home ID onto the device it cannot be changed by means of software [37]. Since Z-Wave adheres to the ITU-T G.9959 specification, devices using this protocol operate in the industrial, scientific and medical bands of the spectrum [14].
For Z-Wave there are three known approaches to classify and exploit vulnerabilities: the radio frequency approach, targeted at the physical layer of the protocol, the gateway approach, set to exploit the gateway controllers, and lastly, the hybrid approach, which covers both of the aforementioned approaches [14].
Kin et al. [10] note in their work how Z-Wave may be vulnerable to DoS, firmware-over-the-air (FOTA), and remote-add mode control if it is set in S0 mode. FOTA describes an attack where the firmware of a device is updated wirelessly. Remote add mode control attack is carried out by an attacker who forces the controller in the Z-Wave network to switch to add-mode (pairing-mode), after which the network key of the victim’s network is intercepted, and the controller forced to pair with the malicious node. Devices must in this mode if they want to connect with each other.

Thread

Thread has been developed by the Thread Group, an Internet of Things standards group that comprises Google's Nest Labs, Samsun, ARM and Freescale [3]. The protocol stack of thread consists of physical and link layer, followed by 6LoWPAN, DVR, UDP and DTLS. Thread has been developed with the application of mesh networks in the home environment [38]. Thread operates on the 2.4GHz frequency range and is built on top of the IEEE 802.15.4 PHY and MAC layers. In a Thread network there are one or more border routers acting as connections to either other Thread networks or external networks [12]. Among the routers in a Thread network, a Leader is elected, which is responsible for keeping a registry of the assigned router addresses and assigning a 2-byte short address to each router in their corresponding network segment. Privacy is protected by forbidding extended unique identifiers (EUI) to be used to address devices that lack the 2-byte short address. Instead, the devices must be addressed using their MAC [12]. The maximum number of supported routers per Thread network amounts to 32 devices, all of them utilizing the next-hop routing method. This means that the routing cost is calculated based on the received signal strength indicator (RSSI) collected from nearby nodes. Thread is not using UDP above the IP layer, instead it uses Constrained Application Protocol (CoAP). CoAP has the purpose of making the exchange of management messages as well as the configuration of multicast addresses on a network possible in a resource constrained setup.

BLE

Is particularly vulnerable to RT/CR MITM attacks, which are carried out after installing Malicious Browser Extensions (ME) on a user's device. These installations are achieved by sending out phishing e-mails. The ME then proceeds to either log the screen or the keystrokes a user performs. With this method, passwords may be obtained among other personal data [39].
The BLE specification defines a complete protocol stack consisting of a physical layer, link layer, Logical Link Control and Adaptation Protocol (L2CAP), Attribute Protocol (ATT) and the Generic Attribute Protocol (GATT).
The protocol stack itself is split into two roles: the Controller and the Host. The Controller dominates physical and link layer while the rest of the stack belongs to the Host.
BLE handles data (eg., storing and accessing), or *attributes*, by using the ATT and the GATT. *Attributes* can be categorized into types, such as *characteristics*, of which those that show similarities are grouped into *services* [18]. *Services* then are the part of the stack that is exposed to connected devices.
Attributes may be marked with either one of three permissions that define how the attribute may be accessed. There are *Attribute permissions*, *Authentication Permissions*, *Authorization Permissions*.
In [18] two vulnerabilities were tested on BLE devices who had co-located Android applications on the same device. In one of the attacks the authors proved that system-wide pairing credentials may be accessed by an adversary. The second attack staged a reuse of connection by the adversary which enabled them to bypass the establishment of a new connection and take a direct route to the server controlling the network [18].
In [40] a proof-of-concept is delivered from the point-of-view of an adversary stating that sniffing BLE connections and tracking them across a network is possible by means of using a suite of real-time algorithms and a tool called Ubertooth One. The tool is capable of listening to the traffic across an entire frequency spectrum, thus putting it into a position where it can capture all devices in range [41]. Furthermore, Ubertooth One may listen to standard Bluetooth packets as well as BLE packets. This, however, is a vulnerability not easily addressed. It takes an intrusion detection system (IDS) to uncover whether a connection has been subject to sniffing over a long period of time.
The three pairing phases in the BLE protocol are explained as follows [42]:

- In Phase One a pairing-request is sent by the initiating device destined for the device it wants to communicate with. The devices will then exchange requirements on authentication, with focus on link key size, I/O capabilities, and bonding requirements. Nothing is encrypted in Phase One.
- In Phase Two the temporary keys are exchanged and then confirmed that each device is using the same key. Is this completed successfully, the STKs are generated using *mrand* values.
- Phase Three is optional and is started after Phase Two is completed and opts to exchange more keys between devices if this fits with authentication agreements made in Phase One.

Bluetooth (and BLE) offers a built-in security feature called "Adaptive Frequency Hopping", sporting 79 channels to enable hosts to jump between frequencies at 1,600 hops per second. Existing

frequencies are excluded from the hops. By utilizing this feature, jamming and interferences are avoided successfully.

In Bluetooth there exists a C0 cipher suite, using stream ciphering and with a length of 128 bits [17].

Devices in a Bluetooth network can be set to “undiscoverable” which prevents them from advertising themselves during a scanning process. BLE without any security features is vulnerable to eavesdropping, downgrading, link key modifications, fuzzing, sniffing, surveillance attacks, DoS, and malware injection. In the following subsections, other attacks found during the research of this thesis are explained shortly.

MAC Spoofing

During the formation of the Bluetooth piconet and before encryption has been established, this attack is carried out. The attacker achieves their goal by impersonating another user and, in this state, can either intercept and modify data or terminate connections altogether.

PIN Cracking

This attack is performed during the pairing process of two devices and their authentication process. The RAND and the BD_ADDR of the target device are collected by the attacker via sniffing. After the successful collection of these values, the PIN is then cracked through brute-force, by running all possible variations of the PIN using RAND and BD_ADDR until the correct PIN is found.

MITM

This attack occurs when devices are attempting to pair. The attack is performed by covertly relaying messages between the devices, thus enabling the attacker to authenticate without a key and making the user believe the pairing was successful.

Bluejacking

Unsolicited messages are sent to a device to trick it into prompting the user to enter an access code, thus enabling the adversary to access files on the target device previously undisclosed to them. Some popular settings for this attack are crowded areas such as airports, shopping malls, trains, and train stations.

Bluesnarfing

This is targeted at mobile phones, hacking them to access data stored in the phone’s memory. Examples for this data are calendars, contacts, images, passwords, and so on.

BlueBugging

For this attack the RFCOMM protocol is exploited. L2CAP plus the base band are used to establish physical connection. The owner of the device is unaware of the attacker connecting to the target device. The attacker gains control of the device through accessing the “AT”-commands (attention commands) sending instructions to the device consequently.

BlueBumping

The handling of link keys is exploited here. Between the attacker and the user, a business card is sent, forcing the user to accept the card, thus creating an authenticated connection. Even if the user deletes the link key, which is an option, a connection to the attacker is still intact. This active connection makes it possible for the attacker to connect to the device later, this time without authentication, simply by requesting new link-key generations.

BlueDumping

In this attack, the attacker spoofs the BD_ADDR of one chosen device to connect with another. The target device requests to authenticate, which is responded by the attacker with “HCI_Link_Key_Request_Negative_Reply”. The attacker sends this because they do not possess a link key at the time. In some scenarios, the targeted device deletes its link key, then goes into pairing mode. This means the attacker can then successfully connect to the device.

Fuzzing

Adversaries cause a target device to behave abnormally through sending non-standard data and malformed packets. The reaction of the device to these packets is observed and vulnerabilities are derived from these observations.

Backdoor

The attacker establishes a trusted relationship with the target device without appearing in the list of trusted devices on said device. Through this relationship, the device’s services and resources are open to the attacker, unbeknownst to the device’s owner.

DoS

In an ordinary DoS attack, an attacker attempts to either crash the network or restart the system by sending packets to the targeted system until it cannot process them anymore due to full memory or bandwidth. Examples for DoS attacks are BD_ADDR duplication, Bluesmack, Bluechop, L2CAP

guaranteed service, battery exhaustion and Big NAK (Negative Acknowledgement). The last attack uses a continuous retransmission loop to attack.

Worm (Cabir Worm, Skulls Worm, Lasco Worm)

During a worm attack, a malicious software sends itself to a target and infects it.

Cabir Worm:
This attack is applicable to mobile phones using the Symbian series 60 interface platform. Here, the user must accept the worm for the attack to succeed. Only then the malware is installed on the device. Users unknowingly accept them because the worms are hidden in applications. Once a device is infected, it can be used by the worm to advertise and spread itself onto other devices.

Skulls Worm:
This is a Symbian Installation System (SIS) trojan file targeting Symbian mobile phones with the same platform as the ones required for the Cabir Worm. For this attack to succeed, the user must install the SIS file. The worm then becomes active. After this, other services to infect are searched and the process repeats itself.

Lasco Worm:
This is a combination of a regular Bluetooth worm and SIS file. The target is the same as for the other two worms mentioned in this subsection. The activation process is the same for the Lasco Worm as it is for the Skulls Worm.

Bluesmack

Bluesmack describes a variation of the DoS attack that is like the “Ping of Death”. The attack is carried out by sending ping packets the size of 600 bytes, parallel to sending L2CAP echo requests to Bluetooth devices. The targeted device crashes due to an overflowing input buffer.

EnOcean

The research process of this thesis has produced no results in the time range defined for the results to be in.

Security Features

In this chapter the security features of the five protocols ZigBee, Z-Wave, Thread, BLE, and EnOcean are analysed in accordance with the sources found during the literature review.

ZigBee

Fields of Application for ZigBee

Zigbee is a wireless standard based on IEEE 802.15.4 specification and is designed to run on low power radio signals [43].
Its fields of application comprise of remote control installations, sensor applications indoors and outdoors, industrial control [13], agriculture automation [13], and environmental Sciences [13].

Included Features and Countermeasures Against Attacks

Karnain et al. [25] present a threat model to address Zigbee network threats prior to listing the attacks. It is divided into several categories of attacks and threats (see chapter “Attacks in the IoT Environment”). This subsection elaborates on the various security features discovered during the research that address these threats.

ZigBee knows three types of devices that can participate in a network: coordinator (ZC), router (ZR), end device (ZED) [44].
When deploying a ZigBee network, one must determine whether it is going to be a) a *centralized* or b) a *distributed* network. These are the two supported topologies for ZigBee. In a centralized network, there is one coordinator, that simultaneously acts as the ZigBee Trust Centre. Its task is to authenticate and join new devices to a network. Contrary to the centralized network the distributed network has no coordinator, but knows at least one router which authenticates new nodes and joins them to the network on successful authentication [44].
The basic security features of ZigBee include a trust centre for securing the integrity of devices in the network and the feature of ACLs [45]. Security services are included in access control, data integrity, data confidentiality, and sequential freshness for replay protection. Details to this procedure are explained by Kao et al. [46]. The security suites in ZigBee comprise AES-CTR to encrypt messages, AES-CBC-MAC to provide secure authentication, and AES-CCM to take care of both, encryption and authentication [46].
MAC layer makes use of AES-CCM 128-bit network key [44] for assuring confidentiality, integrity and authenticity of MAC frames [43]. The network key is shared between devices across the network. The modes of operation in MAC layer cover CTR, CBC and CCM (a combination of CTR and CBC) [12].

Any new device joining the network must provide its MAC address to coordinator for comparison. If a stored authorized MAC address matches the provided address, the device may start communicating. Should the MAC address comparison fail, the requesting device lands on a Black List and is prohibited from further contacting the coordinator [43].

In the Zigbee protocol stack there are three levels of security: non secure mode, ACL, and safe mode.
The safe mode is the best among the three, as it provides ACL and frame load password protection simultaneously.

The *MAC layer* provides three security services: Access control, data encryption, and data integrity. Data encryption is realized by employing the AES 128-bit encryption.
Data integrity is provided through a Message Integrity Code (MIC) [45].

On the *Network Layer* the process of devices joining or leaving the network is handled. The security feature on this layer mentioned in [43] is based on RFID which makes authorized devices tune in on the 2.4 GHz frequency.

On the *Application Layer* there is a sub-layer called ZDO which is, among other functionalities, responsible for tracking the role of devices in a ZigBee network. The ZDO is supported by the APS which provides services the ZDO needs [45]. A proxy firewall has been added on the Application Layer to store active and previously successful established devices [43].

According to An et al. [13] the security functions in ZigBee may be summarized in the following features to ensure users may navigate the network without fear of compromise or theft of personal information:

1. Key establishment
2. Key transfer
3. Frame protection
4. Device management

The key material is shared between the protocol layers, meaning less storage is needed. This is a key advantage on resource-constrained devices [13].

In ZigBee the security mechanism follows 5 major principles [13]:

1. The frame generating layer is responsible for the initial encryption
2. All frames are secured utilizing the network layer
3. On one device all the layers may use the same key
4. Connections are established from end-to-end, meaning only the source device and the target device “speak” with each other
5. All devices in a network are to use the same level of security. This is recommended for the sake of simplicity

Two security levels are possible in the ZigBee protocol: NWK and APS [3], each of which is responsible for securing frames in their own layer (Network and Application layer). On the case of implemented security mechanisms in the Application layer through APS [43] and [13] are congruent. Both furthermore state that APS provides for establishment and maintenance of secure services while ZDO is responsible for device security policies and configurations [43] [13]. APS is furthermore responsible for frame encryption, key establishment, key transport, and device management services.
NWK employs the AES-CCM and creates key and frame counters, the keys must be updated regularly by the TC [47] [37] to guarantee the best possible level of security.
There are three known key types in the ZigBee Trust Centre (TC), the network key, the link key, and the master key. Each network has only one TC which stores and distributes keys and decides whether a new device is allowed to join the network [7]. The master key is shared by more than two devices while the link key is shared only between two communicating devices [45]. It is also master key needed for creation of new link keys. The Network key can be either one of two types: Standard (SNK) or High Security (HSNK) and this key, regardless of its type is shared across the layers. The ZigBee Trust Centre is responsible for the key distribution within the network as well as end-to-end application configuration [45]. All devices use the network key for securing frames and preventing unauthorized devices from using the network, while the link keys are used for sessions between two devices.
The maximum number of nodes that a ZigBee network may mount up to is 65,536 nodes, which makes it the preferable protocol for especially large mesh networks.
In [27] the security levels of the key distribution process are elaborated shortly. There are three identified levels: high level, standard and pre-configured. In high level the NWK is encrypted and then distributed while in the standard level the network key is simply sent over the air without encryption. Is the pre-configured level in place, the NWK is already installed on the device. The security level in a ZigBee network is the same level across all devices. It cannot be changed on a per-frame basis [3].
There are a variety of keys in addition to the three keys mentioned in [7] available in ZigBee [3]:

- Key-transport key
- Key-load key

Both, key-transport, and key-load key are used to secure messages that contain other keys. The key-transport and key-load keys are derived from the link key by utilizing HMAC and the Matyas-Meyer-Oseas hash function. In [12] the newer version of ZigBee (3.0) as well as ZigBee PRO are explained to have a centralized and a distributed mode which newly joining devices are forced to adapt otherwise access to the network is denied.

Z-Wave

Fields of Application for Z-Wave

Z-Wave is a proprietary protocol unlike ZigBee [3]. Z-Wave's fields of application include mainly mesh networks in smart home applications, e.g., controlling lights, switches, dimmers, sensors, and motors [48].

Included Features and Countermeasures Against Attacks

The security of Z-Wave is based on a concept of duality: there are two roles in a network, the controller, and the slave. The controller is the only entity that has full knowledge of the network topology. Among the responsibilities of the controller is the sending of commands to the slave nodes [7].
The slave or child nodes on the other hand can be either one of these two: actuator or sensors. Regardless of the role they hold within a network, slave nodes cannot initiate a communication thread on their own. An explicit command by the controller is required [7]. Slave nodes can forward commands to other nodes if said nodes are not directly reachable by the controller [14]. This message forwarding mechanism is limited to four hops before a packet is dropped by the next node.
Like ZigBee, Z-Wave employs the AES 128-bit in CBC mode (CBC-MAC) [12]. Integrity and authenticity as well as encrypted payload are ensured by Message Authentication Code digest.
The node limit in a Z-Wave network is set to 232 nodes [3] [7].
During the initial set-up the controller and the slaves exchange network keys which are generated by the controller using a pseudo-random hardware number generator (PRNG). This is part of the mode S0, the generation of the network key is described by Kim et al. in detail. After the key has been generated it is stored in the device's non-volatile random-access memory (NVRAM) [10].
From the network key, two more 128-bit keys are derived: a payload encryption key and a data origin authentication key.
Z-Wave makes use of the ECDH Curve25519, working with a 256-bit key length for pairing purposes [48]. The implementation of this encryption makes MITM attacks highly improbable [12].
ECDH, however, is vulnerable to MITM and passive eavesdropping attacks and to counter this, Z-Wave Alliance has implemented three Out-Of-Band (OOB) authentication mechanisms in the security class S2, either of which must be completed by the user to continue the joining procedure [48]:

1. The user enters a PIN consisting of the first 5 numbers of the DSK on the device's outer shell.
2. The user must verify the full DSK by inspecting it
3. The user must scan a QR code to verify the DSK against a trusted server.

After pairing the nodes in the Z-Wave network use symmetric encryption for communication among each other.
The security suite described above is called *S2* and it knows three security classes: "S2 access control", "S2 authenticated", and "S2 unauthenticated" [12]. Each of these classes possess their own

network key, preventing data that has been collected from one class to be decrypted using the key from another class.
S2 is based on 128-bit AES-CCM used for authenticated encryption while AES-128-bit CMAC is used for key derivation functions. S2 can secure key exchanges by utilizing ECDH but must support curve25519 using a public key length of 256 bits. This curve also covers the security requirements dictated by the Federal Office for Information Security in Germany [49].
The security class S2 is furthermore divided into three subclasses, named as follows [5] [49]:

- S2 Access Control
- S2 Authenticated
- S2 Unauthenticated

The security classes have the further purpose of categorizing the devices in a smart home environment into device types: e.g., the first class contains the most trusted devices, the second class the typical smart home devices, and the third class deals with resource constrained devices.
Z-Wave counters MITM attacks by utilizing the entire range of the S2 security suite [5].
Replay attacks are mitigated through exchanging nonce lists.
Global topology state resides in adjacency table, which is maintained by the controller of the network. The table is updated regularly by polling the nodes for their Neighbour List (NL) [16].
The controller generates new routes on demand whenever a node requests to reach a given target. Routing nodes have Source Routing (SR) caches and backbone SR caches needed to reach the controller in addition to NL. The security command class has several restrictions. One, only the message of the application layer is encrypted. Source integrity at the node ID resolution is not possible since all nodes use the same authentication key [16].

Thread

Fields of Application for Thread

The Thread standard covers the entire life cycle of a device within a network. This begins with the device joining a network and ends with the device leaving the network at some point in the future. It has been designed with the IoT use case “Smart Home” in mind and includes building blocks for automation networks.

Included Features and Countermeasures Against Attacks

In Thread, a feature called “Datagram Transport Layer Security” (DTLS) has been implemented. This feature addresses the vulnerability to offline and online dictionary attacks. It also utilizes forward secrecy and know session security [50].
The communication is protected by AES-CCM suite. This suite covers confidentiality, integrity, and authenticity.
It incorporates IPv6 support out-of-the-box due to implementation of IEEE 802.15.4 standard for physical and media access control (MAC). This support is possible due to an additional 6LoWPAN layer, which is integrated between the MAC and the network layer [50] [3].
The protocol stack of Thread covers data confidentiality, integrity, and authentication.
The MAC layer in Thread is securing frames by using a network-wide key to differentiate between a Joiner device and an authenticated Thread device [3]. Joiner devices need to authenticate themselves to gain a trusted position within the network. Otherwise, it is banned from joining. To authenticate themselves they need to find a Joiner Router and initiate a DTLS handshake. The router will then forward all traffic to the Commissioner using a Commissioning relay protocol encapsulating and relaying the DTLS handshake [3]. For detection of neighbours, establishment of secure radio links, and distribution of network keys and PAN ID a Mesh Link Establishment (MLE) handshake is carried out. The network master creates a symmetric master key during network creation and distributes it to all the nodes in the network. Master key of the network must be kept in the non-volatile memory of each node in the network, along with the PAN ID. This allows a node to re-join a network without a user needing to intervene [12]. Once the default key rotation timer of 672h has expired for the master key, the key index number is updated, and a new pair of MAC and MLE keys are created. Thread uses a security feature called Commissioning to counter MITM attacks. To prevent replay attacks, Thread has a key rotation and message sequencing mechanism implemented [5]. Devices that want to join a network for the first time are called Joiners. The device can then transmit an unsecured Discovery Request which is processed by the Joiner Router (JR) and the Router Enabled End Device (REED) and answered with a Discovery Response [22].

BLE

Fields of Application for BLE

BLE has an assortment of applications it has been integrated into, due to its versatility and broad compatibility. Among the most relevant applications are the mobile communications, fitness, and healthcare sector. In mobile communications BLE has been integrated into tablets, smartphones, laptops, and peripherals [51]. Payment systems have been included into the mobile communications sector and can also be found on wearables (e.g., ApplePay). For the fitness sector wearables such as fitness bracelets, rings and smart watches have been introduced. In the smart home sector, BLE can be found in home security systems, energy monitoring applications, home automation and management, and in most smart home electronic appliances (e.g., washing machines, dish washers, coffee makers, smart TVs, thermostats, door locks, …). Recently, the application of asset tracking through BLE has been introduced. Assets can now be tracked and kept under observation.

Included Features and Countermeasures Against Attacks

In the new version of BLE there is the pairing mechanism LE Secure Connections (LESC) which implements numeric comparison as a security feature guarding against eavesdropping and MitM attacks [52] [7] [3]. LESC uses FIPS-compliant Elliptic-Curve Diffie-Hellman for key generation [52]. Kampos-Cruz et al. [53] propose to further increase the level of security by implementing the Curve25519 [54] which also guarantees for a faster key exchange. There are four association models in the pairing mode: Just Works, Passkey Entry, Out-Of-band (OOB) and Numeric Comparison [52] [55] [20]. Passkey entry requires manual user interaction [52].
In addition to the association modes mentioned in [52] the authors of [7] add two Security modes in their analysis of the security features of BLE: Security Mode 1 and Security Mode 2. The former is used at the Link Layer level for encryption and authentication while the latter is focused on unencrypted link layer connections. In Security Mode 2 a 12-byte signature is appended to the payload in the ATT field [7].
There are two BLE paring mechanisms according to [51] and [20]: legacy pairing and Secure Connection (SC). SC was introduced in 2014 and is not vulnerable to MITM and eavesdropping like its predecessor. The reason for this improved security can be found in the new key generation mechanism for LTK: This is used instead of TK. the protocol uses ECDH on the NIST specified P-256 curve [51]. However, SC can only be used if both communicating devices support it.
BLE in general is not advisable as protocol if the device in question is to be part of a mesh network, rather the protocol should be utilized when connecting to a single device, e.g., with a fitness wearable.
In BLE the pairing and bonding, the traffic encryption, and the device address randomization provide security for the devices in a network and protect sensitive data [12].
In the initial paring process, there are three phases to be run through:

- Phase 1 in which the requirements for protection against MITM attacks are exchanged between devices [12]

- Phase 2 in which, depending on the version of BLE, cryptographic keys are created and exchanged between the communicating devices [12]
- Phase 3 in which a protected link is created using the LTK and after that sends the IRK and the CSRK [12].

The MAC addresses in the BLE specification are defined to have four possible types [12]:

- Public
- Static
- Non-resolvable private
- Resolvable private

After two devices have been successfully paired, they need to establish a bond too. This process is initiated by the two devices generating first a temporary key and then proceed to exchange the keys as listed below [55] [3]:

1. A Long-Term Key (LTK) to encrypt data that is sent between two devices. This key must be retained by both devices in case they disconnect at some point and reconnect again, so they do not have to go through the entire pairing process again.
2. Long-term keys remain on the devices unless they are reset or manually unpaired [18].
3. A Connection Signature Resolve Key (CSRK) used by the device on the receiving end to test the integrity of the received data.
4. Identity Resolving Key (IRK) is used to prevent others from tracking the device by constantly generating new random addresses.

The BLE protocol also employs a security feature called AFH, Adaptive Frequency Hopping spread spectrum, which protects an established BLE connection from being sniffed and tracked by adversaries [40]. The parameters for AFH are exchanged during the initial connection establishment. AFH increases the protection against connection tracking by regularly changing the frequency hopping pattern [40].

The BLE protocol version 4.2 fixes the vulnerability of devices against common attacks in Wireless Sensor Networks (WSN) like MITM, passive eavesdropping, and privacy tracking [56]. However, BLE remains vulnerable to battery exhaustion attacks which are designed to intentionally consume battery life of a device and thus, slowly disabling an entire network.

Generally, manufacturers decide which modes of security are included in their devices. Devices will recognize trusted devices using device-level and service-level security.

After successful pairing, a device can invoke more privacy and security provisions. One such provision is whitelisting. The device only connects with other devices it has been paired with previously. All other connection attempts will be rejected [19].

In Bluetooth 4.0, there are the Security Modes 1 to 4, in which all devices capable of Bluetooth operate [17]. The devices may operate in 1 of the 4 four defined modes, each of which sets the available security levels. In a heterogeneous network, where devices are in different Security Modes, downgrading attacks are more likely since a bond needs to be established between devices.

There are also Trust modes in the security features: trusted or untrusted. In a trusted mode, devices have established a fixed relationship and have unrestricted access to services. Contrary to this, the untrusted mode means that the device has successfully passed authentication but has not achieved the fixed relationship, therefor it has restricted access to the services [17].

A device's discoverability can be set to hide its name, class, list of services, and technical information in addition to the BD_ADDR (the equivalent of a MAC address on IEEE 802.x.x devices). Is the device discoverable, this information can be accessed by any adversary [17].

During the initiation of a connection, the authentication between two devices is performed via challenge-response, based on the BD_ADDR and the LK.
Bluetooth 4.0, and consequently BLE, have adaptive frequency hopping as a built-in security feature. This simply means that on the used 2.4 GHz ISM band with its 79 available channels, hops are enabled at a rate of 1,600 hops per second [17].
In BLE devices *Single Mode* can be implemented, and if this is the case, then the device may only communicate with other BLE devices, while classic Bluetooth devices (BR/EDR) are not supported [20].
BLE has in its controller layer a Resolvable Private Addressing (RPA) implemented. RPA's primary concern is the upholding of the secrecy of a BLE device.

On Link Layer five different states are possible [20]:

1. Standby – default state
2. Advertising – advertise to connect to other available devices
3. Scanning – listening for advertisements
4. Initiating – selecting an advertiser, connection is initialised with the other device
5. Connection – data transmission phase

The Link Layer consists of L2CAP, ATT, SM, GATT, and GAP.

L2CAP [20]:
Responsible for the establishment of two devices as protocol multiplexers. This layer encapsulates the protocols from upper layers (ATT and SMP) into BLE packet format. L2CAP is also responsible for SAR.

SM [20]:
Defines the overall security level of BLE. It has two roles: the Security Manager Protocol (SMP) for controlling the pairing mechanism, and the security toolbox, with the primary task of encrypting and decrypting data.
The MAC address is hidden by this layer to increase the overall level of privacy.

ATT [20]:
Client-server stateless low-level protocol necessary for the definition of data exchange between a client and a server.

GATT [20]:
Built on top of ATT, defines BLE libraries, manages how data is formatted and exchanged,
Server has main responsibility of storing data and make it available to clients who request access to it.

GAP [20]:

The highest-level protocol, making the device visible to others. It handles connection establishment and device discovery. Defines roles for each device: central (master), peripheral (slave), broadcaster, observer.
Master devices have high computational power such as smart phones, tablets, and computers. Peripheral devices have less computational power, most of the time these devices are sensors that advertise and connect themselves to a master. Broadcasters are use different channels than other peripherals. Over these channels they receive data from central devices. Observers are central devices and listen for broadcast packets, then initiate connections.

EnOcean

Fields of Application for EnOcean

EnOcean has been designed for sensor networks in industrial and private sectors by the EnOcean Alliance. The protocol mainly uses sub-GHz frequencies, the availability of which depends on the legal regulations of the region it is deployed at.

Included Features and Countermeasures Against Attacks

To make it compatible with ZigBee and BLE systems there exists a solution which has the 2.4GHz band implemented [12]. EnOcean devices can communicate with other networking realms, also ones that work on TCP/IP. However, this communication requires a gateway. Messages are called telegrams in EnOcean and are identified by either the base-ID or a 32-bit chip ID. Telegrams are either secured or they are not, the indicator for this is sent in the R-ORG field of the original message.
AES-128-bit CMAC is used to encrypt the telegrams and provide for the message integrity and authentication of R-ORG S telegrams. To secure P2P communication a rolling code (RLC) may be included in the R-ORG S and this code is incremented with each P2P communication [12]. The receiving device needs to check this code and determine whether to drop the message (the code value is not greater than the last received message's) or receive it (the code value is greater than the previous message's). Further increasing the code's authenticity, it is placed within a window range, to prevent duplication of the code. If the AES key is changed, the RLC value must be set to zero.

Approach, Methods, and Analysis

In this section, the approach to the literature research and analysis is elaborated on. Information is provided on how and why the respective protocols were selected. Then the method for screening and reviewing, called PRISMA, is explained. The platforms, on which the sources are located on, are defined as well as the process of writing the necessary search strings for each platform.
Furthermore, a list of keywords is defined to determine exclusion criteria for reports not deemed suitable to remain in the literature database. The tool to manage the reports and screen them, Zotero, is explained shortly, and how it assisted in the research.
Later in this chapter, the collection of results and the process of screening said results in Zotero is described. The screening process is described in chapter “Keywords for Screening Process” and “Importing Results, Deduplication and Screening”. Prior to the screening process the preparation of the results in the database is elaborated on. The preparation includes the deduplication of search results.

The Protocols Chosen for Analysis

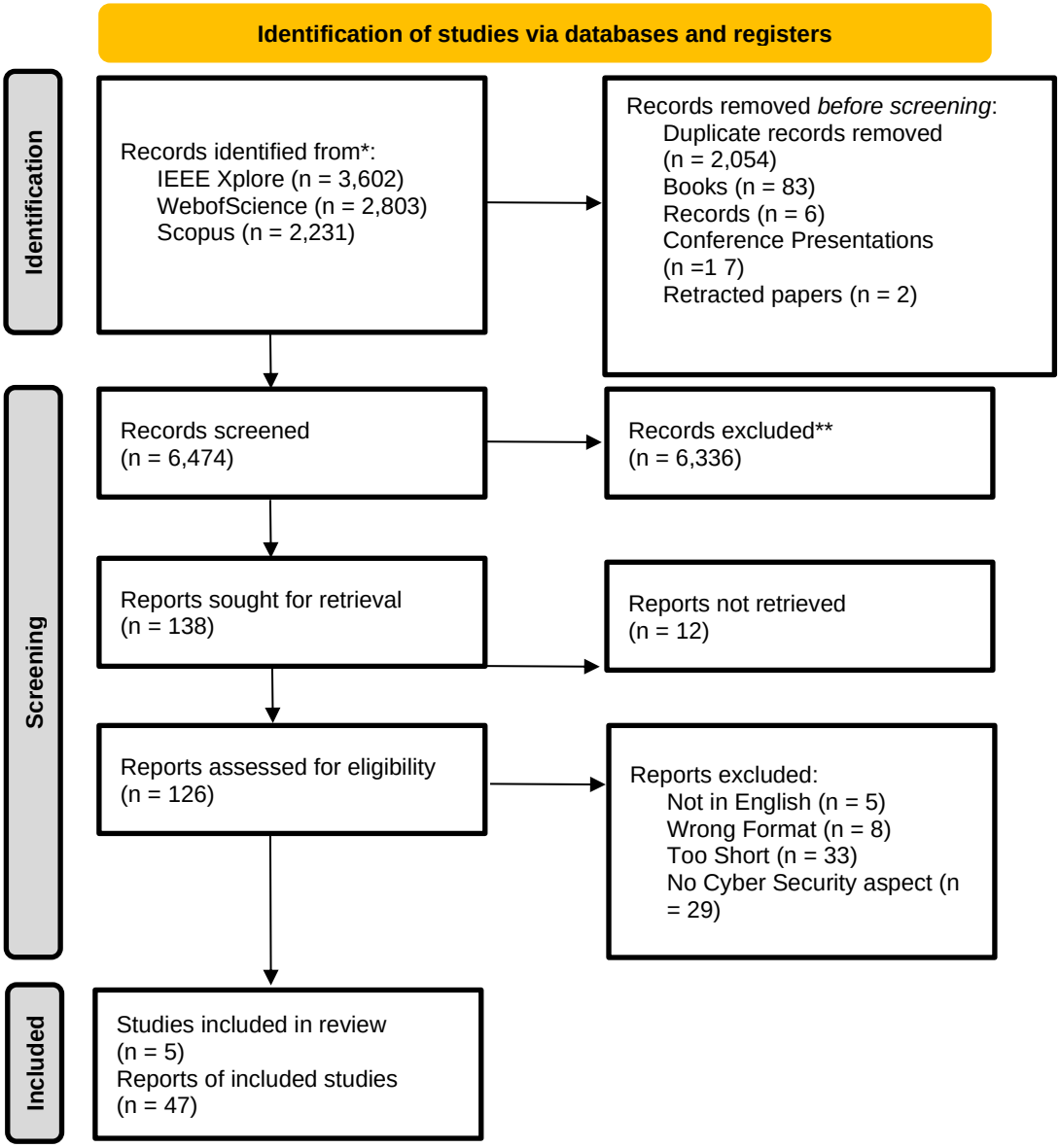
For the literature research and analysis, the most popular and widespread protocols utilized in smart home setups. These protocols were chosen due to their versatility, compatibility, and their usability for end users. Furthermore, it was important to choose protocols that would be usable in apartment complexes where end users often do not have the chance to install the necessary infrastructure for, e.g., KNX.
The protocols that are most popular and have yielded the most results are ZigBee, Z-Wave, Thread, and Bluetooth or BLE. As an additional protocol, though it is less known than its peers, EnOcean is chosen.
A first look on the IEEE platform, the most relevant platform for conference papers in the IT-Sector, demonstrated that the search term “EnOcean” produced 27 results, most of which with little relevance to the topic of this paper. However, the protocol has been included to complete the list. It is recommended to focus on more researched protocols like ZigBee and Thread instead.

PRISMA Method

The Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) statement is a tool that is meant to help authors provide a systematic review that is transparent, coherent, complete, and accurate in its account of why the review was done, what the authors did, and what they found during their research [57]. To achieve this goal, authors can fill out a 27-item checklist, which details reporting recommendations for the items in the list. In addition, an abstract checklist as presented in the PRISMA 2020 statement, and a flow diagram for original as well as updated reviews can be used. For this thesis, the flow diagram was adhered to, since it provided structure, that efficiently advanced the screening process of the research.

The Flow Diagram as Presented in PRISMA 2020 Statement

The flow diagram is categorized into three main parts, which are depicted as blue boxes on the left: Identification, Screening, and Included. The upper two boxes are located at the very beginning of the review process, which in this case, was the identification of the platforms, on which to search for reports. One of the main criteria was, that books, had to be excluded, since most of the information that is up to date is published at considerably shorter intervals than book publishers can manage. The three platforms chosen to search on were IEEE Xplore, WebofScience, and Scopus. The search strings used to produce results are listed and explained in chapter “Keyword Definition for the Search String”. After the initial search, the results have been accumulated into a Zotero database. The process of importing is described in chapter “Importing Results, Deduplication and Screening”. In the first row of the diagram in the top right corner, there is a box that depicts the results of the *pre-screening* process. In this process, duplicates are merged, and thus removed, from the collective dataset. Furthermore, a manual sorting process is carried out, to remove any datasets, that do not fulfil the pre-defined searching criteria. In this case, books, records, retracted papers, and conference presentations have been excluded from future research in this thesis. Retracted papers, conference presentations and records are not peer reviewed publications, and as such, not deemed reliable sources for a systematic review. Books, as mentioned previously, are published at greater intervals between issues compared to journal articles or conference papers, and thus, likely to contain outdated information. Since this is an updated systematic review, sources from before 2016 are excluded from the search and the final database.
The next section in the flow chart deals with the screening process itself. This screening process covered 6,474 items in total (box “Records screened”), after the removal of the items in the top right corner box. Screening was not done in one round, but three, all of which are explained in chapter “Importing Results, Deduplication and Screening”. At the end, 6,336 records were excluded from future research in this thesis (box “Records excluded”). Directly underneath the box “Records screened” the box “Reports sought for retrieval” depicts the number of results (conference papers and journal articles) that were used for a final assessment. This box has a flow arrow pointing to the right to the box “Records not retrieved”. This box describes papers that were not retrievable in the way that they were provided on platforms which required special user accounts or hidden behind paywalls. These paywalls could not be overcome by means of institutional access provided by the University of Applied Sciences St. Pölten. Next in the screening process, and as direct result of the “Reports sought for retrieval” comes “Reports assessed for eligibility”. After the non-retrievable records were removed from the database, 126 records remained for a final assessment. Of these reports, a total of 75 records were excluded for the following reasons (more excluding criteria is provided in detail in chapter “Keywords for Screening Process”). The reports were in a language not readable, and it was unfeasible to translate them. Furthermore, texts being in the category “Conference Paper”, but not in the IEEE approved two column format, were excluded due to lack of credibility. Papers that provided up to four pages of content and were too superfluous were excluded. Lastly, all records dealing with smart home protocols, but not focusing on any security features or cyber security in general, had to be excluded to not being relevant for this thesis.
The final section of the flow diagram, “Included”, presents the number of remaining entries in the Zotero database: 51 reports in total provided content relevant for this review. The results and short notes on their content are listed in chapter “Presentation of Results Table”).



*Consider, if feasible to do so, reporting the number of records identified from each database or register searched (rather than the total number across all databases/registers).
**If automation tools were used, indicate how many records were excluded by a human and how many were excluded by automation tools.

Reports excluded: primary studies were used, other systematic literature reviews were excluded
Reports not retrieved: these were not available (provide a list of titles and authors)

Searching Criteria

As this is an updated systematic review, the searching criteria must include a timeframe to make sure only the most recent reports are included. At the beginning of writing this thesis, which is early 2022, the timeframe is set to search for anything in between 2016 to 2022. Experience has shown that in the sector of cyber security, information technology, and especially in the smart home sector, anything older than 5 (maximum 6 years) contains outdated information.
The main challenge with this review proves to be the vast number of research available due to the size of the field IoT, and smart home. It is also difficult to find a common research terminology because terms like IoT, smart home, or home automation are used synonymously. Other criteria for finding qualitative results were to exclude all books, book chapters, conference presentations, and records. Books and book chapters are excluded because they represent media that is published at great intervals, and once the book or book chapter has been published, information in it has already been overhauled in a conference paper. Conference Papers and journal articles are deemed qualitative sources because they are reviewed by peers before publication and contain current research topics. Each searching process for works covering smart home protocols must produce not more than 2,000 results, 2,300 at most. The reason for choosing this number is simply because anything above would be unfeasible, especially considering that the search is carried out for several smart home protocols, thus the end results will comprise considerably more than 2,000 results.

Keyword Definition for the Search String

To create a search related best to the topic of this thesis and to cover the most ground, a key word list is needed first. This list has been derived in great parts from the work of Kambourakis et al. [12] and is meant as a guide line for the later described search string definition and testing. Not all the words will be used, though, since a longer search string not necessarily produces more results. There is also the matter of character and input parameter limitations on the platforms.

List of Key Words and Possible Search Terms		
Protocol	**Attacks/Weaknesses**	
BLE	User Tracking	Cross-application Tracking
	Activity Detection	Downgrading
	Key Derivation	Eavesdropping
	Person Identification	Replay
	Advertisement Spoofing	Battery depletion
	Exposed Services	Sleep deprivation
	OTP authentication token interception	DoS and DDoS
Z-Wave	Eavesdropping Replay Key derivation Rogue Controller Integrity vulnerabilities of the routing protocol Black hole Unauthorised Commands	
ZigBee	Sinkhole Wormhole User racking Battery drain Key recovery and extraction Key sniffing Network discovery and device identification Jamming Device reconfiguration	

List of Key Words and Possible Search Terms	
Thread	Jamming Flooding Handshake flooding (TCP flooding) Forced network leave Key compromise Replay Same-nonce Guaranteed Time Slot PAN ID conflict DoS and DDoS Side-channel

Table 3: List of key words and possible search terms used for research [12]

Search String Definition, Building Process and Platforms

IEEE Xplore

Search String:

("Document Title":"cyber-security" OR "Document Title":"Wireless Network" OR "Document Title":"Micro?Architecture" OR "Document Title":“Weakness*” OR "Document Title":"Exploit" OR "Document Title":"Side-Channel" OR "Document Title":"key derivation" OR "Document Title":"denial?of?service" OR "Document Title":"wireless protocols" OR "Document Title":"eavesdropping" OR "Document Title":"user tracking" OR "Document Title":"sniffing" OR "Document Title":"Bluetooth?lower?energy" OR "DocumentTitle":"reconfiguration" OR "Document Title":"spoofing")

Conditions:

- Limit to years 2016-2022
- Further limit to conferences, journal, and early access articles
- Results: 3,602

Explanation:

For this search string the syntax needs to be altered, hence the search string for IEEE Xplore looks different from the ones for Web of Science and Scopus.

First, all search terms must be encapsulated in quote signs. Next, the “Document Title” term orders the search engine to look for the quoted keywords within the Title of each result.

On IEEE Xplore there are the following parameters to give the search string as indicator:

- Abstract
- Accession Number
- Article Number
- Article Page Number
- Author Affiliation
- Author Keywords
- Author ORCID
- Authors
- Document Title
- DOI
- Full Text & Metadata
- Funding Agency
- IEEE Terms
- Index Terms
- INSPEC Controlled Terms
- ISBN
- ISSN
- Issue

- Metadata
- MeSH Terms
- Publication Number
- Publisher
- Publication Title
- Standard Number
- Standard Dictionary Terms
- Standard ICS Terms

For this thesis, only the parameter “Document Title” is necessary. Search terms are concatenated using OR, AND, NOT, NEAR or ONEAR. AND an NOT prove to be too restrictive. Instead, OR is chosen to get an appropriate number of results.

The search terms for IEEE Xplore are chosen from the keyword list defined in chapter “Keyword Definition for the Search String” and in the final version of the search string are as follows:

- Cyber-security
- Wireless Network
- Micro Architecture
- Weakness
- Exploit
- Side-channel
- Key derivation
- Denial of Service
- Wireless protocols
- Eavesdropping
- User tracking
- Sniffing
- Bluetooth lower energy
- Reconfiguration
- Spoofing

Some words are separated by “?” instead of a “-“ or “ “. This is because the question mark “?” allows the searching machine to include all variations of the search term, no matter if the words are separated by dash, space, or question mark. The asterisk “*” at the end of the key word “weakness” will produce results regarding anything containing “Weakness”, but through the asterisk, will include any results with words that follow the initial key word.

Web of Science

Search String:

(ZigBee OR (Bluetooth?low?energy OR BLE) OR (z-wave OR Z Wave) OR “EnOcean” OR “thread”)AND (security OR "Wireless Network" OR "Micro?Architecture" OR Weakness OR Exploit OR “Side-Channel” OR “key derivation” OR “denial?of?service” OR “wireless protocols” OR

“eavesdropping” OR “user tracking” OR “sniffing” OR “reconfiguration” OR “spoofing” OR “ipv6” OR “WPAN” OR “privacy attack*” OR “botnet*” OR “attack* surface” OR “replay attack*”)

Conditions:

- Limit to years 2016-2022 and conferences and articles
- Limit to subject area computer science and engineering and decision science
- Number of results: 2,803

Explanation:

For Web of Science, the syntax of the search string is a slightly different one, than for IEEE Xplore. In example, no parameter like “Document Title” or “Abstract” is necessary. Instead, parenthesis to enclose the search terms are used and concatenated using Boolean operators, such as AND, OR, and NOT [58]. The search string consists of one encompassing parenthesis construct, with many smaller compounds. These compounds (also bordered by parenthesis) contain the most likely and sensible variations of a chosen search term. For example, during a first scouting of available research, the protocol BLE has appeared either directly referred to as “BLE” or “Bluetooth Lower Energy”. This variation is encapsulated in parenthesis, and “Bluetooth Lower Energy” is separated by question marks. Just as on IEEE Xplore, the question mark enables the search engine to look for results no matter the separator between the words, so long as the result contains the three words “Bluetooth lower Energy”. The same principle works for the asterisk used at the end of one given search term. The asterisk suggests that what comes either before or after the search term is unknown, but it may be there, and the result will still be relevant. In such a case, a journal article may appear in the results, containing more words than the search term has, but due to the asterisk, this is allowed and a valid result. AS with IEEE Xplore, the usage of the Boolean operator AND as well as NOT is not recommended, as both restrict the number of results in a way that less than 100 remain. This applies to all platforms: IEEE Xplore, Web of Science, and Scopus. Since Web of Science’s search engine is not as complex as Scopus or IEEE Xplore, limitations of results need to be set on subject areas only. For this thesis, computer science, engineering and decision science are the best matches.

Scopus

Search String:

(ZigBee OR (Bluetooth?low?energy OR BLE) OR (z-wave OR Z Wave) OR “EnOcean” OR “thread”)AND (security OR "Wireless Network" OR "Micro?Architecture" OR Weakness OR Exploit OR “Side-Channel” OR “key derivation” OR “denial?of?service” OR “wireless protocols” OR “eavesdropping” OR “user tracking” OR “sniffing” OR “reconfiguration” OR “spoofing” OR “ipv6” OR “WPAN” OR “privacy attack*” OR “botnet*” OR “attack* surface” OR “replay attack*”)

Conditions:

- Publication years: Limit to years 2016-2022
- Document types: Limit to articles, proceedings, papers, review articles, early access

- Research areas: Further limit computer science, engineering, telecommunications, science technology other topics, automation control systems, remote sensing
- Language: Limit to language English
- Number of results: 2,231

Explanation:

For Scopus just like for Web of Science, the syntax of the search string is slightly different to that of IEEE Xplore. For example, no parameter like “Document Title” or “Abstract” is necessary. Instead, parenthesis are used to enclose the search terms, and concatenated using Boolean operators, such as AND, OR, and NOT [58]. The search string consists of one encompassing parenthesis construct, with many smaller compounds. These compounds (also bordered by parenthesis) contain the most likely and sensible variations of a chosen search term. For example, during a first scouting of available research, the protocol BLE has appeared either directly referred to as “BLE” or “Bluetooth Lower Energy”. This variation is encapsulated in parenthesis, and “Bluetooth Lower Energy” is separated by question marks. Just as on IEEE Xplore, the question mark enables the search engine to look for results no matter the separator between the words, so long as the result contains the three words “Bluetooth lower Energy”. The same principle works for the asterisk used at the end of one given search term. The asterisk suggests that what comes either before or after the search term is unknown, but it may be there, and the result will still be relevant. In such a case, a journal article may appear in the results, containing more words than the search term has, but due to the asterisk, this is allowed and a valid result. AS with IEEE Xplore, the usage of the Boolean operator AND as well as NOT is not recommended, as both restrict the number of results in a way that less than 100 remain. This applies to all platforms: IEEE Xplore, Web of Science, and Scopus.

The limitations must be refined gradually, starting with the type of publication preferred for the results. In this case, articles, proceedings, papers, review articles, and early access works are the preferred outcome.

On Scopus, the limitation of results must be expanded on research areas, since Scopus is a platform that is publishing across the branches of various scientific, therefor, publications are not exclusively focused on engineering, cyber security, communication technologies or IT. Furthermore, any language a published work is written in other than English, is not viable for this thesis.

Keywords for Screening Process

This chapter contains a list of keywords or phrases that were used during the screening process, which means during the sorting out of the over 8,000 items in the Zotero database described in chapter “The Flow Diagram as Presented in PRISMA 2020 Statement”.

Screening Round	Keyword(s)/excluding criteria
1 Screening Headlines for indicators that fit the topic	■ Smart grid, smart agriculture, smart healthcare ■ Cyber security in traditional networks ■ Protocols not containing “ZigBee, Z-Wave, Thread, BLE or EnOcean” ■ Electronics Engineering ■ Signal analysis ■ Sector not smart home or IoT ■ Language not English
2 Screening Headlines for finer nuances of wording that fits the topic	■ Improving efficiency or throughput ■ Not smart home related ■ Not cyber security related ■ Deals mainly with IPv6 ■ Performance, throughput, enhancing connectivity ■ Home security systems and their implementations (because cyber security and home security are not the same) ■ Smart vehicles or smart cars
3 Screening Headlines AND Abstracts to determine if content is suited	■ Implementing smart sensor networks in dense environments with lots of interferences, challenges with that ■ Near-field communication with no relation to smart home or internet of things ■ Cloud computing with no relation to smart home integration or internet of things ■ Forensic analysis of collected data from IoT networks ■ Introducing new frameworks for creating a smart home network with no focus on cyber security ■ Position determination of moving objects in either public open spaces, indoor, a car or similar

Screening Round	Keyword(s)/excluding criteria
	■ Home security systems and their implementations (because cyber security and home security are not the same)

Table 4: Number of screening rounds and key words used for screening and excluding items

Importing Results, Deduplication and Screening

After the search strings ran through the three platforms IEEE Xplore, Web of Science, and Scopus, the results had to be exported into a format that could be processed by Zotero. For Zotero to be able to interpret the results, they need to be in RIS data format (Research Information System). On Web of Science and Scopus, the files can be extracted all at once into one RIS-file.
On IEEE Xplore only the entries displayed on one page can be exported. The solution to that involves more steps than on Web of Science, including to set the number of entries displayed on each site to the maximum value possible on IEEE Xplore: 100. After this is done, all the 100 displayed items can be exported by selecting them. This task is then repeated until all results are done exporting, which in this case comprise 3,602 files in total. This resulted in 37 RIS-files which store the results from the IEEE Xplore search.
The RIS-files from all three platforms are then imported in Zotero and extracted. This method allows to display all the metadata of each search result as seen in Figure 8.

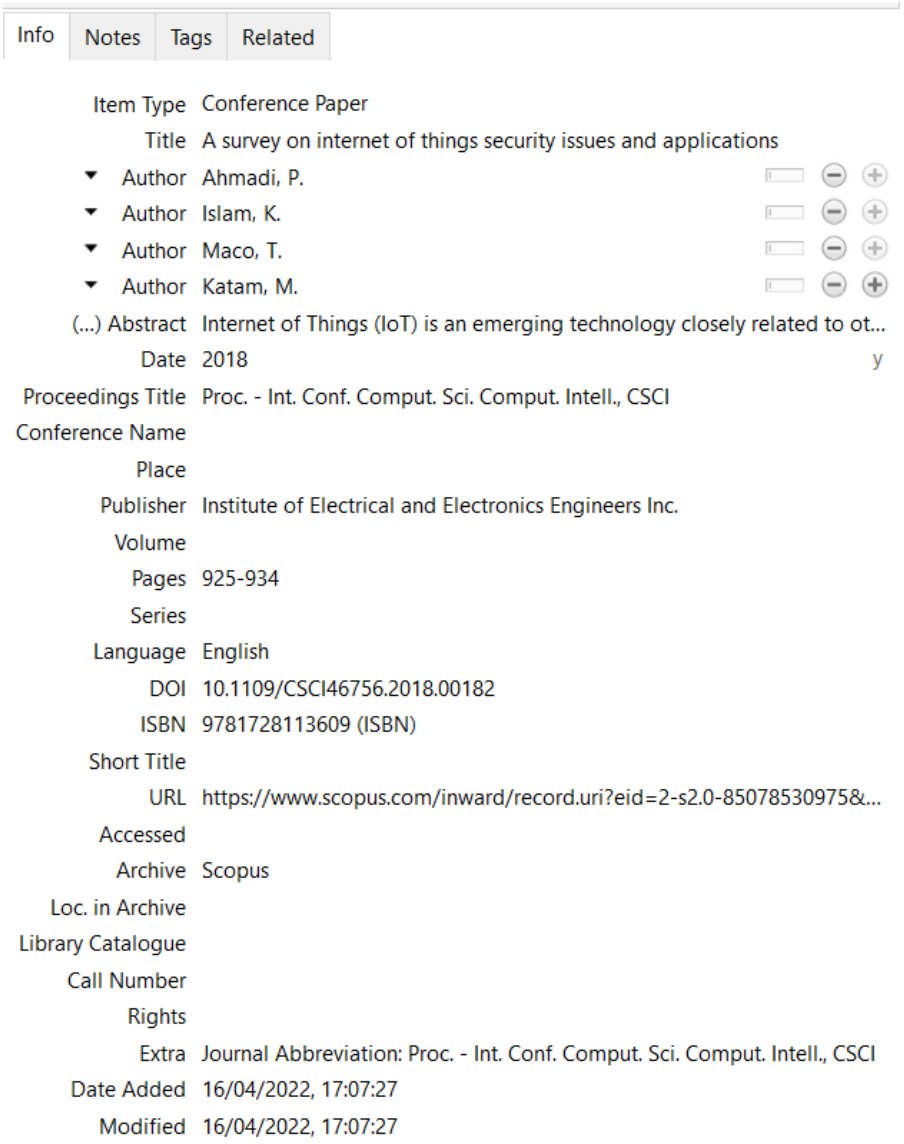


Figure 8: Example of how Zotero displays the metadata of entries in the database

After all the RIS-files are extracted, the double entries need to be merged. During this process 2,054 entries turned out to be double entries. Prior to the merging there were 8,636 items in total. After merging and sifting out rogue entries (for more information on this, see chapter “The Flow Diagram as Presented in PRISMA 2020 Statement”) 6,474. There are entries holding the same title, but according to their metadata are of different “type”, e.g., a journal article holds the same title as a chapter in a book. These entries then cannot be merged. Therefore, one of each must be deleted manually as part of the screening process. This concerned 197 entries in total. If there are three items, one is a conference paper, the second is a journal article, and the third is a book, the book must be deleted. Afterwards the remaining two entries can be merged without conflict. All the deduplicated entries are collected in one library file, called “deduplicated results”.
The sorting process consisted of removing and merging duplicates as far as possible. What remained was then sorted again keeping in mind that anything containing the keywords (s. chapter “

Keyword Definition for the Search String") from the literature search or lacking the context needed for this analysis must be deleted. After the first screening 952 items remained in total. The first screening focuses on the titles of the search results only with the key words from chapter "Keyword Definition for the Search String" serving as guidance.

The second screening will again remove all results that do not focus on smart home technology, e.g., keywords such as smart farming or smart healthcare do not fall into the focus of this work.

All works that are centred around industrial IoT setups are excluded as well. Same goes for courses that focus solely on introductions into cyber security and secure architectures without providing context to IoT.

After the second screening, which eliminated all results connected to smart cities, smart grid, smart agriculture, smart healthcare, and cyber security without IoT context the remaining items amounted to 749 in total.

The third screening focuses on the elimination of search results based on title AND abstract. Papers and publications must be centred around smart home setups or smart home setups and user experience. All end results must be concerned with at least one or more aspects of cyber security, be it user privacy, establishing secure connections, protection against attackers, testing for vulnerabilities or implementing device and/or user authentication mechanisms.

Further exclusion criteria are centred around works that have one or more of the following topics at its core: energy efficiency, enhanced data throughput, data transmission methods.

Also excluded from the database were all papers where the abstract did not give sufficient information about the content of each paper (e.g., five-lines-abstracts were eliminated).

Results of Literature Analysis

State of Research

The most recent studies that provide an oversight of security features concerning IoT protocols, or synonymously called “smart home protocols” and “Wireless PAN protocol stacks” are written by Kambourakis et al. (published 2020) [12] and Tournier et al. (published 2021) [37].
Kambourakis et al. [12] analyze the security feature of the protocols BLE, ZigBee, Thread, Z-Wave, and EnOcean in their work, and they do an in-depth analysis. Since their study was published in 2020, it offered up-to-date insight on the current smart home protocols and their security features. Their review also covered attacks that are related to the respective security features. Furthermore, the authors provide an overview of key security issues in WPAN protocols. The authors have included works that present new frameworks and security tools in their review as well.
The coverage of important features like Confidentiality, Message Authenticity & Integrity, Anti-Replay, MITM protection, and Device authentication is presented in form of a table. The table includes footnotes to highlight conditions which must be met to successfully cover the security feature. The chapters focusing on security features are elaborated in detail and in reference to the works the authors analysed. Other than that, no structure is adhered to in the chapters. The table the authors presented is not brought into relation with the content of the security features themselves. It is therefore not possible to create a connection between the presented security features and where in the table these can be placed. EnOcean is not represented in the literature review as there exists no specific work addressing the security features of EnOcean, a condition that has not changed in this updated literature review. The authors defined a time frame in which the results of their survey must have been published, spanning from 2013 to 2019. Furthermore, the IEEE 802.15.4 header is explicitly covered in a separate chapter, which this work does not do. IEEE 802.15.4 is part of the protocol stacks of ZigBee and Thread and is therefore included in the respective chapter that covers the protocol stacks. Users are passively protected by the security mechanisms listed, and not participating actively in the achievement of improved network security; this task is left to the developers and manufacturers. In another chapter the security features in context with corresponding attacks are analysed, although there is no layer specific focus visible in the structure. A second table is presented which lists published works per type of attack and linked to the respective protocol (e.g., BLE). They then continue to analyse what was published in the works they listed, omitting some of the works listed, and adding one attack specific work to the analysis that was not mentioned previously in the table. There is no mention of how the authors came upon the resulting works of their review which they analysed. It is unclear, where these works have been taken from, what was used to find them, and how the authors have managed to curate a manageable amount of works to analyse amid the vast pool of available literature (meaning, the screening process is not comprehensible).
Tournier et al. [37] have conducted a three-tier survey through the lens of a generic IoT stack. The authors cover the protocols OS41, BLE, ZigBee, Z-Wave, Wirelesshart, LoRaWAN, SigFox. The first group of the survey focused on the security of each specific protocol stack. The second group

covered the comparison of protocols, specified on one OSI layer. The third group addressed a global view of security and associated challenges in IoT. The authors compare protocol stacks according to their range, openness, interoperability, network architecture, security practices, and the generic IoT stack. They continue to present the features of each stack categorized into range, openness, interoperability, types of topology, security practices. Finally, the authors study not only IoT attacks, but also in reference to packet security, protocol security, and system security. Lastly, Tournier et al. do not describe the method used to arrive at the collection of results they chose to analyse. It is unclear, where they found their sources, how they found them, and how the screening process was carried out.

Presentation of Results Table

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
Li Li, P. Podder, E. Hoque	A Formal Security Analysis of Zigbee (1.0 and 3.0)	Develop a model for Zigbee 1.0 and 3.0 and demonstrate security properties	Conference Paper	2020	Zigbee 1.0/3.0	Zigbee, protocol verification, cryptographic keys, symmetric encryption, providing secrecy of messages	Replay attacks, Man-in-the-Middle, Sniffing	Frame Counters, Regularly updated Keys	No
K. J. Campos-Cruz, C. Mancillas-López, B. Ovilla-Martinez	A Lightweight Security Protocol for Beacons BLE	Discussing the main security threats for applications that utilize BLE beacons, and introducing a security protocol for establishment of shared secrecy keys	Conference Paper	2021	BLE	BLE, IoT, beacons, Security, lightweight cryptography for resource constrained devices, BLE Beacon Protocols iBeacon, Eddystone and Altbeacon, Diffie-Hellman (ECDH) protocol with cure 25519	Beacon forgery, unauthorized tracking, beacon spoofing, showrooming, impersonation	Shared Secret through ECDH with curve 25519	no
Yu Liu, K. A. Hassan, M. Karlsson, Z. Pang, S. Gong	A Data-Centric Internet of Things Framework Based on Azure Cloud	Proposing a data-centric IoT framework incorporating three protocols with fundamental security schemes (WiFi, Thread and LoRaWAN)	Journal Article	2019	Zigbee, Thread, WiFi, LoRaWAN	Azure Cloud, Peripheral services, function services, edge computing, communication standards, secure network joining and leaving, encryption of data in transit on resource constrained devices	Offline dictionary attack, KRACK, radio jamming	WPA3, Forward secrecy, DTLS, AES-CCM,	yes
P. Sivakumaran, J. B. Alis	A Low Energy Profile: Analysing Characteristic Security on BLE Peripherals	Presenting an open-source profiler meant to classify and determine the protection level of data at rest on BLE devices	Conference Paper	2018	BLE	Bluetooth Standard, Pairing modes, Association models, Authenticated and unauthenticated keys, Profiler, dictionary attacks	passive eavesdropping, unautorised data access on device, MitM, data modification	numeric comparison	yes

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
G. Varshney, M. Misra, P. Atrey	A New Secure Authentication Scheme for Web Login Using BLE Smart Devices	Comparison of existing authentication schemes to identify research gaps, proposing a new authentication scheme using BLE, BT 4.0+	Conference Paper	2017	BLE	real time (RT) / control relay (CR) Man-in-the-Middle attack (MITM), phishing, malicious browser extensions, Bluetooth, authentication schemes	RT/CR MITM, address spoofing, key stroke logging, screen logging, password sniffing, phishing	Hardare Token, Usage of Bluetooth hardware address (BTADDR) of BLE (BT 4.0+)	yes, partially (entering a PIN code for authenticated key generation)
A. B. Karnain, Z. B. Zakaria	A Review on ZigBee Security Enhancement in Smart Home Environment	Ranking security attacks on a ZigBee network and evaluating their severity, additionally proposing countermeasures to make ZigBee networks more resilient, presenting a threat model for categorization of threats to a ZigBee network	Conference Paper	2016	ZigBee(N/A)	Wireless Sensor Networks (WSN), Machine-to-Machine communication(M2M), Network Threat Model, Network attacks, Attack severity classification, ZigBee	eavesdropping, DoS, node compromise, sinkhole and wormhole attacks, physical attack	Authentication scheme with encyption algorithm where XOR calculation is performed twice and protects agains active and passive attacks, Using a new key distribution scheme when a node joins a ZigBee network preventing MITM (Diffie-Hellman parameter exchange integrated into handshake), utilizing Zigbee's Received Signal Strength (RSS) to prevent spoofing	no
J. H. Biddut, N. Islam, R. S. Sultana, A. Sarker, M. M. Rahman	A New Approach of Zigbee MAC Layer Design Based on Security Enhancement	Enhancing the security of ZigBee by modifying the MAC layer of the protocol, improving network and application	Conference Paper	2016	ZigBee	Zigbee Network, Improved Security on MAC layer, device registration process by comparing stored MAC addresses	none	MAC address authentication, RFID Detection, Application Security	no

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
		security, providing end-to-end security, block unauthorized sensor nodes on MAC level							
Y. Tang, H. Lian, L. Li, X. Wang, X. Yan	A Randomness Detectin Method of Zigbee Protocol in a Wireless Sensor Network	Proposing a randomness detection method of Zigbee protocol intended to appraise whether the protocol has encryption mechanisms and encryption strength	Journal Article	2018	ZigBee	Zigbee network, random sequence number, cryptography, matrix propability test, symmetric cryptography (AES)	none	Frame Encryption, security policies, end-to-end encryption, symmetric encryption	no
D. Celebucki, M. A. Lin, S. Graham	A Security Evaluation of Popular Internet of Things Protocols for Manufacturers	Identifying security features and shortcomings of IoT Protocols, helping manufacturers decide whether to invest in development of a proprietary protocol or opting for one of the three presented	Conference Paper	2018	Zigbee, Z-wave, BLE	Trust Centers, Key management, ZigBee, Z-Wave, BLE, security features and vulnerabilities, exploits on IoT devices	jamming, compromised layers go undetected, sniffing, traffic analysis, key extraction, battery depletion, replay attack	MAC authentication, Key regeneration, symmetric cryptography, key rotation, up-to-date hardware, anti-tampering	no
Amiruddin, A. A. P. Ratna, R. F. Sari	A Testbed Implementation of Secure and Lightweight Privacy Preservation Mechanism Using Scrambled	Proposing a lightweight privacy preservation mechanism with a new key generation, combining modified Fibonacci and	Conference Paper	2017	ZigBee	encryption, fibonacci, privacy preservation, ZigBee exploits, IEEE 802.15.4, attacks on protocol layers, methods of attacks, attack targets, network member or non-member	KillerBee, AVR RZ USBstick, communication interception, energy depletion	Offering a new way to encrypt the keys in a ZigBee network	no

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
	Fibonacci and XOR for ZigBee	symmetric and asymmetric cryptography							
M. V. Katam, T. Maco, K. Islam, P. Ahmadi	A Survey on Internet of Things Security Issues and Applications	Outlining the security, privacy and identity and architecture design of IoT, recommending approaches to address these concerns	Conference Paper	2018	ZigBee	Internet of Things, smart cities, architecture design of IoT, privacy issues, data protection, attack landscape, ZigBee, security vulnerabilities, IAS-octave, CIA principles,	node capture, malicious code injection, false data injection, replay attack, cryptoanalysis attacks, side channel attacks, eavesdropping, sleep deprivation, DoS, spoofing, sinkhole, wormhole, MITM Routing Information attack, unauthorized access, Sybil attack, phishing, malicious scripts, worms, viruses, exploiting cryptographic weaknesses	?	no
S. Teerakanok, T. Uehara, A. Inomata	A Secure Cloud-centric IoT Framework for Smart Device Registration	Proposing a generic framework for IoT device registration, Security and user-friendliness are main points of the paper, along addressing countermeasures to attacks like eavesdropping, MITM, replay	Journal Article	2021	BLE	registration processes, shared-secret exchange, close-range communication registration by using NFC or RFID, 6-step process to registrate devices	eavesdropping, replay attacks, modification, MITM	not discussed	yes

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
S. Cha, M. Chuang, K. Yeh, C. Su, Z. Huang	A User-Friendly Privacy Framework for Users to Achieve Consents with Nearby BLE Devices	Proposing a user-friendly framework for users called PrivacyBat, defines specifications for users to get to an agreement on privacy, provide guidelines for a device so it can process user request, deliver proof-of-concept, define a secure and consent-based registration process	Journal Article	2018	BLE	BLE, Privacy, pairing mechanisms, bonding procedure between devices, exchanging keys, random addresses, tracking prevention, PrivacyBat	brute force, eavesdropping, key derivation,MAC address obtainment, user tracking, replay attacks	random address scheme, data signatures, integrity checks, encrypted data transfer, counters, strong user authentication	yes
D. Dragomir, L. Gheorghe, S. Costea, A. Radovici	A Survey on Secure Communication Protocols for IoT Systems	Providing a survey of networking stacks for IoT with special focus on security capabilities, taking into account industry alliances and standardization bodies	Conference Paper	2016	IEEE 802.15.4, WiFi,NFC, LoRaWAN, Z-Wave, BLE, Thread, ZigBee, 6LoWPAN, RPL, IPSec, CoAP, MQTT, XMPP, AMQP	NFC Forum, ZigBee Alliance, Thread Group, LoRa Alliance, network stacks, security features of IoT protocols	traffic interception, data injection, traffic sniffing	message freshness, data origin authentication, network keys, payload encryption, counters, low frequency, end-to-end communication	no
P. Sivakumaran, J. Blasco	A Study of the Feasibility of Co-located App Attacks against BLE and a Large-Scale Analysis of the Current Application-Layer Security Landscape	Presenting how unauthorized co-located Android applications can access pairing-protected BLE data, present mitigation strategies with focus on various stakeholders,	Conference Paper	2019	BLE	BLE devices, stack description, co-located apps, unauthorized access to protected data, encryption, key generation, pairing processes, BLECryptracer, AttackApp scanner	unauthorized data access, shared credential stealing, connection reuse, exploiting API calls, malicious application overwrites	protecting data at higher layers, key rotation, regular firmware updates	yes

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
		introduce BLECryptracer to identify presence of application-layer security							
S. Sarkar, J. Liu, E. Jovanov	A Robust Algorithm for Sniffing BLE Long-Lived Conenctions in Real-time	Point-of-View of the adversary, develop a suite of real-time algorithms to determine parameters needed to sniff a BLE connection	Conference Paper	2019	BLE	connection sniffing and tracking, indoor environment tracking, pairing processes, real-time algorithm implementation, Ubertooth One application	packet injection, sniffing, connection tracking, jamming	intrusion detection systems	no
P. M. L. An, T. Kim	A Study of the Z-Wave Protocol: Implementing Your own Smart Home Gateway	design and implementation of Z-Wave gateway for smart home system, discuss limitations of protocol	Conference Paper	2018	Z-Wave	implementation of smart home gateway, Z-Wave protocol, IoT, wireless network, user interaction	none	none	no
S. Sevier, A. Tekeoglu	Analyzing the Security of Bluetooth Low Energy	test the security features of the BLE protocol as defined in the respective standard, by exploiting the vulnerabilities	Conference Paper	2019	BLE	Ubertooth One, sniffing, encryption breaking with Crackle	sniffing, encyrption breaking, DDoS, replay, handshake capture	none	none
K. Narayanan	Addressing the Challenges Facing IoT Adaptation	Discussing challenges a business may face when adapting its environment to support IoT applications	Journal Article	2017	NB-IoT, Cat-M, Z-Wave, ZigBee, SIGFOX, LoRa, ANT, Thread, Wi-SUN, WiFi	battery drain, radio formats, power integrity, signal integrity, business models, hybrid environments, home networks	none	none	none
B. Fan	Analysis on the Security Architecture of	elaborate on ZigBee security architecture,	Conference Paper	2017	ZigBee	access control lists, ZigBee, Trust Center, IEEE 802.15.4, key	none	frame counter, updated network	none

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
	ZigBee Based on IEEE 802.15.4	services, model, components, keys and the Trust Center, highlight security features on each layer				management, key sharing, frame protection, counter		keys, high security keys	
G. Kambourakis, C. Kolias, D. Geneiatakis, G. Karopulos, G. M. Makrakis, I. Kounelis	A State-of-the-Art Review on the Security of Mainstream IoT Wireless PAN Protocol Stacks	providing a comparison of the smart home protocols ZigBee, Z-Wave, BLE, Thread and EnOcean	Journal Article	2020	ZigBee, Z-Wave, BLE, Thread, EnOcean	IoT, Security, WPAN, IoT protocols, literature review, attack listing, ZigBee PRO, certificate based authentication	MITM, eavesdropping, key leakage, MAC frame replay, impersonation, spoofing, tampering, package injection, token interception, DoS, downgrading, jamming, battery drain, sniffing	frame counter, device identification, Master key, using non-volatile memory, device chip ID	none
J. Tournier, F. Lesueur, F. Le Mouel, L. Guyon, H. Ben-Hassine	A Survey of IoT protocols and their security issues through the lens of a generic IoT Stack	describing a generic approach to tackle the security challenges in IoT, comparison of IoT stacks BLE, ZigBee, WirelessHart, define comparison criteria according to openness, range, interoperability, network architecture, security practices	Journal Article	2021	ZigBee, BLE, WirelessHart, LoRaWAN, SigFox, NB-IoT	generic IoT stack, OS4I stack description, security in Z-Wave, BLE, ZigBee, LoRaWAN, WirelessHart, SigFox	MITM, buffer overflows, Spoofing, Sybil, wormhole, sinkhole, selective forwarding	common security criteria, harmonising security, constant security level	none

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
K. Lounis, M. Zulkerinine	Attacks and Defenses in Short-Range Wireless Technologies for IoT	doing a survey of attacks on wireless protocols available in IoT setups, categorized into fabrication, interception, modification, interruption, and domination attacks for WiFi, Bluetooth, ZigBee, and RFID	Journal Article	2020	ZigBee, WiFi, Bluetooth, RFID	IoT Security, WiFi, Bluetooth, ZigBee, RFID, security in WPANs, attack classification, countermeasures, security features, attack-defense trees	rogue acknowledgement, packet injection, replay, physical attack, side channel, network discovery, same-nonce, sniffing, frame trashing, geedy behavior attack, battery exhaustion, end-device sabotage, PAN-ID conflict, guaranteed time-slots attack, CSMA/CA exploit, jamming	authentication mechanisms for management frames, management frame protection implementation, bit-stuffing, timestamps, data freshness, IDS, key invalidation on intrusion, anti-temper measures, masking, cross-copying, conditional assignment, bucketing, predictive timing mitigation, AES, OOB channels, device watcher	none
S. N. Swamy, S. R. Kota	An Empirical Study on System Level Aspects of Internet of Things (IoT)	presenting current state of functional pillars of IoT, summarizing architecture of IoT, providing the current status of communication standards and application layer protocols used in IoT, emphasizing on analysing security challenges, privacy and security threats, mitigation techniques	Journal Article	2020	RFID, BLE, ZigBee, Z-Wave, Thread, LoRaWAN, NB-IoT, Sigfox, 5G, Telensa, Ingenu	pillars of IoT, usecases of IoT, fields of application for IoT, emerging IoT applications, requirements, architecture, edge computing, fog computing, cloud computing, security threats, privacy threats, cloudlets, IoT platforms	spoofing, MITM, node replication, DoS, DDoS, tag cloning	lightweight cryptography, hardware security, intrusion detection and prevention system (IDPS)	none

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
S. Pallavi, V. A. Narayanan	An Overview of Practical Attacks on BLE Based IoT Devices and their Security	demonstrating possible attacks on the BLE protocol using various tools to perform spoofing, MITM and firmware attacks	Conference Paper	2019	BLE	pairing process, nordic thingy, attacks, data capture, fitness tracker	spoofing, MITM, firmware attack	fingerprinting, secure connections, authenticated connecting points, integrity checks, official updates, user education	yes
Z. Guo, I. G. Harris, Y. J., Lih-feng Tsaur	An Efficient Approach to Prevent Battery Exhaustion Attack on BLE-based Mesh Networks	presenting an intrusion detection and prevention approach for Battery Exhaustion Attacks aimed at BLE devices	Conference Paper	2016	BLE	threat model, Battery exhaustion attacks, vulnerability fixes, scatternet, priority lists, defense approaches	battery exhaustion, MITM, DoS, eavesdropping, privacy tracking	implementing BLE 4.2, blacklisting nodes	none
S. Marksteiner, V. J. E. Jiménez, H. Vallant, Herwig Zeiner	An Overview of Wireless IoT Protocol Security in the Smart Home Domain	presenting an overview of application domains for IoT, discussing wireless IoT protocols KNX-RF, EnOcean, ZigBee, Z-Wave and Thread, describing security features of protocols and compare with each other	Conference Paper	2017	ZigBee, Z-Wave, EnOcean, Thread, KNX-RF	curve25519, ECDH, security features, protocl stacks, OSI layer model, IoT application fields, star topology, fully connected topology, mesh topology	none	none	none
M. B. Yassein, W. Mardini, T. Almasri	Evaluation of security regarding Z-Wave wireless protocol	researching vulnerabilities on Z-Wave and pointing out ways for administrators to secure their Home Area Networks (HANs)	Conference Paper	2018	Z-Wave	Z-Wave protocol stack description, encryption, security vulnerabilities and mitigations, frame	packet injection, weak authentication, MITM, rogue controller injection	Hide WLAN SSID, robust passwords in WLAN administration, MAC address filtering, reverse proxy server implementation, log file inspection	none

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
M. Lilli, C. Braghin, E. Riccobene	Formal Proof of a Vulnerability in Z-Wave IoT Protocol	offering a formal verification of the security of the Z-Wave protocol, focusing on the join procedure of nodes into a network	Conference Paper	2021	Z-Wave	ASMETA formal framework, join procedure exploitation, S2 security class, OOB authentication mechanisms, security features	MITM, passive eavesdropping, packet injection, password cracking	OOB authentication, Device Specific Keys, QR code verification,	yes
X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, J. Chen	Ghost-in-ZigBee: Energy Depletion Attack on ZigBee based Wireless Networks	investigating a severe attack on ZigBee protocol called ghost, showing how deploying standard suite of security mechanisms does not protect against the ghost, proposing countermeasures to withstand and localize the ghost in the network	Journal Article	2016	ZigBee	security architecture, WSNs, IEEE 802.15.4 specification, integrity, confidentiality, attack design, adversary detection, forming of networks, nodelist and ACL	ghost, energy depletion, DoS, jamming, sleep deprivation, spoofing, eaves dropping, replay attack, nonce reuse	periodic sleep and wake up phases	none
I. Unwala, Z. Taqvi, J. Lu	IoT Security: Z-Wave and Thread	looking at security challenges for an IoT System, discussing different types of attacks on the protocols	Conference Paper	2018	Z-Wave, Thread	security challenges, authentication, privacy, physical security, confidentiality, data integrity, trust, authorization, local attacks, protocol stacks	MITM, DDoS, sinkhole, black-hole, selective forwarding, router map, version number, replay, third party attack	nonce exchanging, key rotation	none
P. Morgner, S. Mattejat, Z. Benenson, C. Müller, F. Armknecht	Insecure to the Touch: Attacking ZigBee 3.0 vie Touchlink Commissioning	warning about further adoption of the commissioning mode in ZigBee 3.0, analyzing the security of touchlink commissioning procedure,	Conference Paper	2017	ZigBee 3.0	ZigBee 3.0, IoT, network models, threat models, security, penetration testing framework	DoS, spoofing, reset to factory-new attack, permanent disconnect, hijack, network key extraction	none	yes

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
		presenting novel attacks, releasing an open-source penetration testing framework							
D. Antonioli, N. O. Tippenhauer, K. Rasmussen	Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy	demonstrating the vulnerability of Bluetooth and BLE to key negotiating downgrad attacks employing standard-compliant downgrade attacks	Journal Article	2020	BLE	key exchange procedures, key negotiation, security, mobile device attacking, UberTooth	key negotiation downgrade attack, entropy downgrade, MITM, brute force	require higher minimum entropy value for LTK, distrust the BLE link layer, employ BALSA at application level for security guarantees	yes
J. D. Fuller, B. W. Ramsey, M. J. Rice, J. M. Pecarina	Misuse-based detection of Z-Wave network attacks	extending an existing implementation of Z-Wave MBIDS and providing a side-by-side comparison through an experiment examining the accuracy of misuse detection in both the baseline and the extended MBIDS implementation	Journal Article	2017	Z-Wave	Z-Wave, WSNs, vulnerability analysis, misuse detection, experimental setup, radio frequency approach, gateway approach, hybrid approach	packet injection, key reset, impersonation	none	yes

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
T. Choudhury, A. Gupta, S. Pradhan, P. Kumar, Y. S. Rathore	Privacy and Security of Cloud-based Internet of Things (IoT)	analyzing and comparing the threats a cloud-based IoT environment faces	Conference Paper	2018	none	cloud computing, cloud devices, edge computing, cyber attacks, IoT, nodes, storage security	injection, information leakage, replay, tampering, cloning, capture gateways, physical capture, congestion, node replication, forwarding, jamming, eavesdropping, DoS	encryption either asymmetric or symmetric,	none
M. Grabovica, D. Pezer, S. Popic, V. Knezevic	Provided security measures of enabling technologies in Internet of Things (IoT): A Survey	exploring security protocols used in IoT: RFID, ZigBee, Wifi, and Bluetooth, presenting possible issues that could occur in a practical appliance	Conference Paper	2016	Bluetooth, ZigBee, RFID, WiFi	RFID, wireless sensor networks, data security, network layers, ZigBee protocol layers, Bluetooth vulnerabilities, RFID attacks	tampering, packet sniffing and injection, key leakage, bluejacking, bluesnarfing, clandestine scanning and tracking, skimming and cloning, exploiting cryptographic weaknesses	protected device memory, protect default TC links, key rotation	yes
K. Fawaz, K.-H. Kim, K. G. Shin	Protecting Privacy of BLE Device users	analyzing existing BLE privacy measures and how they fare in real-world deployments using an assortment of collected data	Conference Paper	2016	BLE	scanning, advertisement, BLE, BLE-Guardian, threats, Commercial-Off-The-Shelf (COTS) hardware, user intervention, whitelisting	identity tracking, sniffing, address spoofing, profiling	device hiding, access control	yes
S. R. Hussain, S. Mehnaz, S. Nirjon, E. Bertino	Seamless and Secure Bluetooth LE Connection Migration	proposing a new system for seamlessly and securely migrating BLE connections after the initial	Conference Paper	2017	BLE	gateway, BLE, connection, trusted pairing, threat model, transferring connection state, pairing-bonding, privacy, stack cloning,	gateway spoofing, unauthenticated packet injection, sniffing, modifying packets	establish subsequent gateways in the network, give variables and connection state information to	no

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
		gateway went out of range				full stack and half stack cloning		them, secret group keys, verify public key certificate	
A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd	Security Vulnerabilities in Bluetooth Technology as used in IoT	presenting an overview of Bluetooth technology in IoT setups, including an analysis of its security, vulnerabilities, threats, and risk mitigation solutions, providing real-life examples of exploits	Journal Article	2018	BLE	Bluetooth 1,2,3, and 4 protocol stacks, security threats, vulnerabilities, exploits	eavesdropping, spoofing, PIN cracking, breaking encyption, downgrading, link key modification, fuzzing, malware injection, MITM, sniffing, surveillance, DoS, BlueJacking, BlueSnarfing, BlueBugging, BlueBumping, BlueDumping, BluePrinting, Blueover, BlueBorne, Offline PIN recovery, bruteforce, relay, backdoor, worm, Bluesmack, MultiBlue, HeloMoto, Bluecasing, War Nibbling, Car Whispering	enhancing user awareness, keeping devices in range, long random PIN codes, undiscoverable mode, software updates, minimal pairing, combination keys, link encryption for all data transmission, mutual authentication, encrypting broadcasts, maximum encryption key size, use security mode 3	yes

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
A. Barua, MD A. A. Alamin, MD. S. Hossain, E. Hossain	Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey	presenting a comprehensive taxonomy for the security and privacy issues of BLE, possible attack scenarios for different types of vulnerabilities, classifying them according to severity, listing mitigation techniques	Journal Article	2022	BLE	BLE, vulnerabilities, passive eavesdropping, fingerprinting, privacy attack, IoT, wearable device, security tools, connection phases 1-3, pairing methods	active and passive eavesdropping, device cloning, MITM, replay, sniffing, DoS, PIN cracking, authentication attack, battery exhaustion, denial of sleep, jamming, distortion, fuzzing, Blue-Smack, fingerprinting, activity detection, Blue-Printing, Blue-Stumbling	secure connection, numeric comparison, OOB, minimum Passkey entry, secure and private environment, data encryption with AES 128-bit, MITM flag specification if I/O capabilities exist, nonces, random session key, passwords, RPA, white- and blacklist, increase TK length, random BD_ADDR, multi-layer authentication, energy signature monitor, request number threshold, L2CAP implementation	yes
M. C. Francisco, S. Eisa, M. L. Pardal	Secure protocol buffers for Bluetooth Lower Energy communication with wearable devices	presenting POSE, an end-to-end security layer, which can mitigate attacks on BLE apiring and link-layer communications	Conference Paper	2021	BLE	IoT, BLE, security, privacy, POSE, protocol buffers	eavesdropping, MITM, downgrade attacks, DoS	encryption, payload verification	no
E. A. Asonye, I. Anwuna, S. M. Musa	Securing ZigBee IoT Network Against HULK Distributed Denial of Service Attack	investigating the HTTP Unbearable Load King (HULK) DDoS attack using a ZigBee network as reference, the goal to	Conference Paper	2020	ZigBee	HULK DDoS attack, SVM, KNN, RF, NB, IoT, ZigBee	HULK DDoS	source client obfuscation, reference forgery, stickiness, no-cache	no

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
		implement a security method using Support Vector Machine (SVM), Random Forest (RF), Naive Bayes (NB), and K-Nearest Neighbor (KNN)							
H. Pirayesh, P. K. Sangdeh, H. Zeng	Securing ZigBee Communications Against Constant Jamming Attack Using Neural Network	proposing a ZigBee receiver leveraging MIMO technology, capable of decoding a desired signal despite the constant presence of jamming attack	Journal Article	2021	ZigBee	IoT communication, jamming, physical-layer security, ZigBee networks, radio communication	jamming	neural network for jamming mitigation	no
D.-G. Akestoridis, M. Harishankar, M. Weber, P. Tague	Zigator: Analyzing the Security of ZigBee-enabled Smart homes	presenting a security analysis tool, Zigator, for in-depth study of ZigBee networks, study security consquences, develop attacks to test	Conference Paper	2020	ZigBee	security and privacy, mobile security, WSNs, smart home environment, security investigation tool, experimental setup, ZigBee Protocol Stack, threat model design, testbed implementation	jamming, spoofing, packet injection, packet sniffing, network reconnaissance, key transport attacks	improving commissioning process of network devices	no
R. Cayre, F. Galtier, G. Auriol, V. Nicomette, M. Kaaniche, G. Marconato	WazaBee: Attacking ZigBee networks by diverting Bluetooth Low Energy chips	discussing the security of IoT communication protocols, presenting a new attack called WazaBee, aimed at BLE devices, presenting key principles of the attack	Conference Paper	2021	BLE, ZigBee	WazaBee, ZigBee, BLE, IoT networks, attacks, IEEE 802.15.4, pivotal attacks, signal modulation to interpret a signal sent by a different protocol on ZigBee device	WazaBee	implement cryptography acc to IEEE 802.15.4	no

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
C. W. Badenhop, Scott R. Graham, B. W. Ramsey, B. E. Mullins, L. O. Mailloux	The Z-Wave routing protocol and its security implications	reverse engineering the frame forwarding and topology management aspects of the Z-Wave protocol, performing a security analysis to identify source and data integrity vulnerabilities, conducting a Black Hole attack	Journal Article	2017	Z-Wave	pairing operation, reverse engineering, SDR, security analysis, network management, command classes	Black Hole, passive collection, frame injection, impersonation, NL modification, SR cache modification	mandatory use of security commanc class, use asymmetric node authentication	yes
L. Babun, H. Aksu, K. Akkaya, E. S. Bentley, A. S. Uluagac	Z-IoT: Passive Device-class Fingerprinting of ZigBee and Z-Wave IoT Devices	proposing a new fingerprinting framework called Z-IoT, used to identify device classes in ZigBee and Z-Wave protocols	Conference Paper	2020	ZigBee, Z-Wave	fingerprinting ZigBee and Z-Wave devices, network-based fingerprinting, fingerprinting IoT devices, threat model, packet capture, packet filtering, feature extractor, signature generator, classifier	spoofing, injection, unauthorized access	fingerprinting framework Z-IoT	no
T. Nallusamy, R. Ravi, G. Sathiyaprabhu	Virus Propagation in Hetergeneous ZigBee Networks with Human Behaviours	developing a virus propagation and prevention model for heterogeneous IoT networks, calculating factors like virus propagation in networks as well as human behaviour into the concept	Conference Paper	2016	ZigBee	network scanning, discoverable and invisible modes, Cabir virus, file sharing, model development, propabilities, human behaviours, compartment models	brute force, proximity scanning		yes
F. Farha, H. Ning, S. Yang, J. Xu, W. Zhang, K.-K. R. Choo	Timestamp Scheme to Mitigate Replay Attacks in	proving that security feature (frame counter) in ZigBee is insufficient to	Journal Article	2022	ZigBee	replay attack, mitigation strategy, ZigBee network, ZigBee End Devices	Replay attacks, Man-in-the-Middle, Sniffing	enhanced timestamp scheme	no

Authors	Title	Purpose	Type of Source	Year	Protocols	Major Themes	Attacks/threats Mentioned	Countermeasures Proposed	User Interaction
	Secure ZigBee Networks	counter replay attacks, mitigation strategy design for all ZigBee topologies and states of end devices				(ZEDs), enhanced timestamp schemes			
M. Ren, X. Ren, H. Feng	Z-Fuzzer: Device-agnostic Fuzzing of Zigbee Protocol Implementation	developing a device-agnostic fuzzung platform to detect vulnerabilities in ZigBee devices and network implementations	Conference Paper	2021	ZigBee	fuzzing, security, vulnerability detection, ZigBee, protocol stack	fuzzing		no
K. Kim, K. Cho, J. Lim, Y. H. Jung, M. S. Sung, S. B. Kim, H. K. Kim	What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol	examining threat modeling using the STRIDE model on the Z-Wave protocol, determining the security issues, suggesting attack scenarios to gain control of commercially available Z-Wave products, analyzing level 2 data flow diagram of products, presenting results of experiment	Journal Article	2020	Z-Wave	Z-Wave, Wireless sensor networks, STRIDE threat model, threat modeling, IoT, smart home, smart city	DoS, Firmware-over-the-air (FOTA), remote add-mode control	use security level S2, symmetric keys	no

Table 5: Presentation of results of Literature Review sorted alphatecially according to authors

Discussion

The state of research was such that although the presentation of the technical content was done thoroughly, the method as to how the works the authors have analysed have been acquired are not mentioned anywhere. There is no hint, as to the platforms that were searched, specific keywords that the authors used or omitted and how they screened the pool of results once the search has been conducted. With this thesis the screening method as presented by PRISMA 2020 is utilized to provide better transparency and replicability.

Group BLE

Campuz-Cruz et al. [53] focus on the main security threats for applications that utilize BLE beacons by introducing a security protocol that helps establishing shared secret keys. In this way they contribute to an enhanced security suite for the entire protocol.
Sivakumaran et al. [52] have a unique approach to security in BLE: they present an open-source profiler with the aim of classifying and determining the current supported security level in the target devices. This tool makes it possible to find potential weaknesses in a network and set goals to gradually upgrade certain devices which may now not support the latest security features. These legacy devices prove to be a great risk factor for a network's overall security as the newer devices which could implement up-to-date features have to be "downgraded" to meet the legacy device's needs, otherwise the two would be incompatible.
In their work Varshney et al. [39] compare existing authentication schemes to identify research gaps primarily, and secondarily, propose a new authentication scheme designed for BLE and Bluetooth 4.0+. Their authentication scheme is targeting one specific threat: RT/CR MITM attack. They are the only authors addressing an issue this particular with BLE networks.
Teerakanok et al. [6] propose a generic framework for IoT device registration centred around cloud technology. The focus of their work lies on user-friendliness and security, next to addressing countermeasures to well-know attacks such as eavesdropping and MITM attacks. The authors elaborate registration processes of devices and put special attention to close-range communication registration through usage of NFC or RFID and the arising security concerns connected to it. Their contribution is a 6-step registration process for devices. The authors focus specifically on BLE in their setup.
Sivakumaran et al. [18] have focused entirely on BLE and connecting it to Android applications which have it implemented. In their work the authors demonstrate how unauthorized co-located Android applications can access pairing protected BLE data. They furthermore present mitigation strategies with focus on various stakeholders. Finally, their contribution includes a new tool, called BLECryptracer, which has the purpose of identifying the presence of application-layer security on said Android applications.
Sarkar et al. [40] also cover BLE exclusively, though from the Point-of-View (PoV) of the adversary. They developed a suite of real-time algorithms to determine parameters needed to successfully sniff

a BLE connection. The authors focus on connection sniffing and tracking, indoor environment tracking, pairing processes, and real-time algorithm implementation. They use Ubertooth One to conduct their research and are the first authors in this updated review who utilized it in the context of BLE.

Sevier et al. [41] focus on the security of BLE and they analyse it by testing the security features of the protocol as they are defined in the respective standard. Their tests are realized through exploitation of vulnerabilities. This reverse approach to testing how effective BLE security features are, is unique among the works chosen to be used in this thesis.

Pallavi et al. [42] focus on practical attacks on BLE based IoT devices and the security implications of such. They demonstrate possible attacks using various tools which carry out spoofing, MITM and firmware attacks. Alongside Ubertooth the authors also use Nordic Thingy to conduct their experiments.

Guo et al. [56] have chosen to tackle the security issue by introducing an ID/IP approach targeted at battery exhaustion attacks aimed at BLE devices. Their work includes a threat model, priority lists for their tools, vulnerability fixes, and defence approaches. In this they are among a few authors among the pool of works who provide a solution to a specific attack.

Antonioli et al. [51] focus on the traditional Bluetooth protocol as well as on BLE in their work about key negotiation downgrade attacks. They demonstrate the vulnerability of Bluetooth and BLE to this attack by carrying out standard-compliant downgrade attacks. They are the only authors in the entire selection of analysed works who focus on key negotiation downgrade attacks.

Fawaz et al. [19] analyse existing BLE privacy measures for protection of the users and how they fare in real-world deployments. The authors use an assortment of collected data to achieve this. One of the tools the authors work with is called BLE-Guardian. For their experiments they use Commercial-Off-The-Shelf (COTS) hardware.

Hussain et al. [59] propose a new system propose a new system for seamlessly and securely migrating BLE connections after the initial gateway went out of range. They are the only authors who discuss a secure migration of connections. One of their measures for securing the migration included a trusted pairing, transferring the connection state, cloning the stack, and introduce pairing-bonding. They achieve their motive by establishing subsequent gateways in the network, giving variables and connection state information to them, creating secret group keys, and verifying the public key certificates of the devices.

Lonzetta et al. [17] present an overview of Bluetooth technology in IoT setups, and included an analysis of its security vulnerabilities, threats, and risk mitigation solutions. The authors further provide examples of possible exploits such as eavesdropping, spoofing, PIN cracking, breaking encryption, and many more. Their list of attacks is the broadest among the selection of papers in this review.

Barua et al. [20] present a comprehensive taxonomy for the security and privacy issues of BLE. They discuss possible attack scenarios for different types of vulnerabilities and classify them according to severity. Finally, the authors list mitigation techniques for the attacks. In their work they cover the BLE connection phases 1 to 3.

Francisco et al. [60] present POSE, an end-to-end security layer which can mitigate attacks on BLE pairing and link-layer communications. In this, they are the first to introduce a new layer to achieve security goals.

Cayre et al. [21] discuss the security of IoT communication protocols and present a new attack called WazaBee. This attack is aimed at BLE devices which are used in a field experiment to demonstrate key principles of the attack.

Group ZigBee

Li et al. [47] discuss in “A Formal Security Analysis of ZigBee (1.0 and 3.0) how they developed a model specifically for ZigBee 1.0 and ZigBee 3.0 with the purpose of demonstrating the security properties not only of the protocol but each version. This provides a good overview on the improvements the developers made in version 3.0 for better network security and stability.
Kamain et al. [25] have chosen to rank security attacks on a ZigBee network and evaluate their severity. They do not elaborate on security features primarily, but they do come consequently to the previous identification of attacks. Their security measures are presented as countermeasures to the attacks with the goal of making ZigBee networks more resilient. They furthermore present a threat model to help categorizing attacks and the threat they pose to a network, which in turn simplifies the process for selecting counter measures to attacks.
Biddut et al. [43] focus on enhancing only the security of one specific layer in the ZigBee protocol stack, namely the MAC layer. They do so by slightly modifying the MAC layer, thus improving the security of network and application. Through their modification, the authors establish end-to-end security and introduce a mechanism to block unauthorized sensors in the network directly on the MAC layer. This mechanism relieves the upper layers of the protocol stack from performing this mechanism, leaving more room for other services.
Tang et al. [13] take encryption functionalities of ZigBee into account by submitting a randomness detection method for the ZigBee protocol stack with the intention of appraising whether the protocol has encryption mechanisms and determine the strength of the encryption in place. They do not explicitly focus on any known weaknesses of the protocol or potential threats to a network’s security, but they do suggest utilizing several encryption mechanisms on the MAC layer. The authors chose to carry out their randomness detection through a matrix probability test.
Amiruddin et al. [27] introduce a concept for a lightweight privacy preservation mechanism utilizing a new key generation method for ZigBee. Their method is highly mathematical compared to other works, as they combined modified Fibonacci with symmetric and asymmetric cryptography. The author’s approach addresses several mentioned attacks and provides a possible solution through one way.
Fan [45] has conducted an analysis on the security of ZigBee and on a broader spectrum on the IEEE802.15.4 header which this protocol is based on. The author elaborates on the security architecture, services, model, components, keys, and the ZigBee Trust Centre. The security features are highlighted on each layer they apply to, which provides for a better readability of the paper. Specific attacks are not mentioned, the work is entirely focused on presenting security features.
Ahmadi et al. [5] only outline the security, privacy and identity as well as architecture design and recommend various approaches to address all the concerns connected to these areas. Their contribution consists of expanding the well-known CIA triangle of classic cyber security concerns into the IAS-Octave. This octave covers not only the three principles of the CIA triangle but consists of areas that specifically target a heterogeneous ZigBee network and its needs for security and privacy.
Lounis et al. [35] do not do a survey of security features in a smart home protocol but they survey attacks on wireless protocols available in IoT setups. These attacks are categorized into fabrication, interception, modification, interruption, and domination attacks. Their surveyed protocols are WiFi,

Bluetooth, ZigBee, and RFID. The authors are the only ones in this updated review that focus first on an attack landscape and provide suggestions for countermeasures second.
Cao et al. [46] chose to investigate on a severe attack on the ZigBee protocol called “Ghost”, which is able to bypass the standard suite of security mechanism provided by the protocol specification. The authors propose a set of countermeasures to withstand and localize the Ghost in the network, as the main challenge with this attack is to detect it in the first place. The authors provide a great insight into the attack and why it is so sinister and dangerous to a network. They make a point of describing the best countermeasures, insisting that standard level security will not live up to protect the network from an infiltration by the Ghost.
Morgner et al. [44] have put the spotlight on ZigBee 3.0 and how to carry out an attack on it via touchlink commissioning. The authors contribute by warning developers about the further adoption of the commissioning mode in ZigBee 3.0. In an experiment they analyse the security of the touchlink commissioning procedure, present novel attacks and release an open-source penetration testing framework. Morgner et al. are the second group of authors focusing on a specific version of the ZigBee protocol for their work.
Asonye et al. [61] focus on the unique HULK attack, an attack ZigBee networks have been found vulnerable to. The authors investigate the HTTP Unbearable Load King (HULK) attack using a ZigBee network as reference. The goal of the authors was to implement a security method using Support Vector Machine (SVM), Random Forest (RF), Naïve Bayes (NB), and K-Nearest Neighbor (KNN). They are the first authors that implement machine learning in their analysis of the attack.
Pirayesh et al. [62] propose a ZigBee receiver leveraging MIMO technology. Their receiver can decode a desired signal despite the constant presence of a jamming attack.
Akestoridis et al. [63] have developed a security analysis tool called Zigator, with the purpose of studying ZigBee networks in-depth. The authors study the security consequences and develop attacks to test.
Babun et al. [64] propose a new fingerprinting framework called Z-IoT and they use it identify device classes in ZigBee and Z-Wave protocols. ZigBee and Z-Wave devices are fingerprinted on a network-basis. Then a signature is generated.
Farha et al. [65] deliver proof that the security feature frame counter in ZigBee is insufficient to counter replay attacks. The authors have therefore designed a mitigation strategy design for all ZigBee topologies and states of end devices.
Ren et al. [66] have developed a device-agnostic fuzzing platform to detect vulnerabilities in ZigBee devices and network implementations.

Group Thread

Hassan et al. [50] propose a data-centric IoT framework incorporating three protocols with fundamental security schemes: WiFi, Thread, and LoRaWAN. They discuss cloud architectures as they are found in networks utilizing Azure as their product of choice. The main concern of the authors are the security mechanisms that regulate a device’s secure joining and leaving of a network. They are among the only ones focusing on cloud-architectures and peripheral services in their work.

Group EnOcean

Marksteiner et al. [49] present an overview of application domains for IoT, discussing wireless IoT protocols KNX-RF, EnOcean, ZigBee, Z-Wave, and Thread. For these protocols the authors give a description of security features of protocols and compare them with each other. They put strong emphasis on cryptography, narrowing down on ECDH curve25519 which is especially cost-efficient for small devices. Their discussion includes the use cases of mesh networks, fully connected topologies, and star topology.

Group Z-Wave

An et al. [9] also conducted a study, but of the Z-Wave protocol and how to implement a smart home gateway by yourself. Another core topic of their work are the limitations of the Z-Wave protocol. In their work, the user as an active participant in the smart home environment is indirectly referenced.
Yassein et al. [15] have researched the vulnerabilities of Z-Wave and pointed out ways for administrators to secure their Home Area Networks (HANs). The authors give a description on the Z-Wave protocol stack, its encryption mechanisms, the security vulnerabilities, and mitigation techniques.
Lilli et al. [48] delivered a formal verification of the security of Z-Wave, focusing on the join procedure of nodes into a network. Their work is built on the ASMETA formal framework, a set of tools around the Abstract State Machines (ASMs). The tools in ASMETA are aimed to support different activities of the system development process, and help reusing information about models by other researchers. The authors execute an exploitation of the join procedure, elaborating on the advantages of the S2 security class, suggesting OOB mechanisms to secure a network, and, lastly, explain security features. Their decision to work based on a framework designed to give transparency and repeatability produced results that are superior in quality to those of other researchers.
Unwala et al. [22] have analysed the security of Z-Wave and Thread, pointing out the security challenges an IoT System faces, and discuss different types of attacks on the protocols. Their analysed attacks included classic MITM and DDos as well as more unconventional attacks like sinkhole, blackhole, and selective forwarding.
Fuller et al. [14] have extended an existing implementation of Z-Wave MBIDS and provided a side-by-side comparison through an experiment examining the accuracy of misuse detection in both the baseline and the extended MBIDS implementation. They do not provide any suggestions for countermeasures in their work.
Badenhop et al. [16] have reverse engineered the frame forwarding and topology management aspects of the Z-Wave protocol, and performed a security analysis to identify source and data integrity vulnerabilities. The authors have conducted a Black Hole attack to produce the desired results for their reverse engineering.
Babun et al. [64] propose a new fingerprinting framework called Z-IoT and they use it identify device classes in ZigBee and Z-Wave protocols. ZigBee and Z-Wave devices are fingerprinted on a network-basis. Then a signature is generated.
Kim et al. [10] examined threat modelling using the STRIDE model on the Z-Wave protocol and determined the security issues. The authors suggest attack scenarios to gain control of commercially available Z-Wave products and then analyse level 2 data flow diagrams of said products. Their results are presented in their experiment.

Group Miscellaneous

Celebucki et al. [7] have chosen several IoT protocols and provide a security evaluation of popular IoT protocols. Their target are the manufacturers of devices for the IoT sector. The authors have chosen to evaluate ZigBee, Z-Wave, and BLE. In their work they focus on security features and corresponding shortcomings of the protocols, thus assisting the manufacturers in their choice of security features for their devices. The evaluation is also intended to help manufacturers in the decision on whether to invest in the development of a proprietary protocol.
Cha et al. [55] propose a user-friendly framework for users called PrivacyBat which defines specifications for users to get to an agreement on privacy. The authors provide guidelines for a device so it can properly process a user request. Furthermore, the authors give a proof-of-concept to their framework and define a secure and cosent-based registration process.
Dragomir et al. [3] have conducted a survey of networking stacks for IoT with special focus on security capabilities, taking into account industry alliances and standardization bodies. Their work discussed a wide range of protocols with each of them providing a very good overview of each protocol. The protocols the authors have covered, include IEEE802.15.4, WiFi, NFC, LoRaWAN, Z-Wave, BLE, Thread, ZigBee, 6LoWPAN, RPL, IPSec, CoAP, MQTT, XMPP, and AMQP. For each protocol defense mechanisms and security features have been mentioned, including message freshness, data origin authentication, network keys, payload encryption, counters, low frequency, end-to-end communication.
Narayanan [38] on the other hand addresses the challenges that have to be faced when adapting IoT in a business. This author is the first to focus on entire business environments in his work, not simply the manufacturer branch or software developers for IoT applications. In his work, he covers a variety of IoT protocols such as NB-IoT, Cat-M, Z-Wave, ZigBee, SIGFOX, LoRa, ANT, Thread, Wi-SUN, and WiFi. The author does not address specific security features in his work, only the general technical information and limitations of each protocol.
Kambourakis et al. [12] provide another comparison of mainstream IoT protocols such as ZigBee, Z-Wave, BLE, Thread, and EnOcean. Their approach is entirely theoretical and focuses on IoT, security and how it is implemented in WPANs. Additionally, the authors list several relevant attacks tailored to the various protocols under discussion.
Tournier et al. [37] describe a generic approach to tackle the security challenges in IoT environments. They do a comparison of the protocols BLE, ZigBee, and WirelessHart sorting their results into five groups: openness, range, interoperability, network architecture, and security practices. They are the first authors to define criteria which are then used to compare the features of each protocol and provide structure to the reader.
Swamy et al. [2] have done an empirical study the current state of functional pillars of IoT, they then summarize the architecture of IoT, and provide the current status of communication standards. The authors elaborate on the application layer protocols used in IoT, putting emphasis on analysing security challenges and threats to privacy and security. As a final contribution the authors list mitigation techniques. Their covered protocols include RFID, BLE, ZigBee, Z-Wave, Thread, LoRaWAN, NB-IoT, Sigfox, 5G, Telensa, and Ingenu.
Choudhury et al. [23] are among the authors who analyse and compare threats a cloud-based IoT environment has to face. They do not address any specific IoT protocols though. In their work the

authors discuss possible attacks especially on edge devices and how to implement better storage security. Their discussed attacks include injection, information leakage, replay attacks, tampering, cloning, capture gateways, physical capture, node replication, jamming, eavesdropping, and DoS.
Grabovica et al. [36] have conducted a survey on the provided security measures of enabling technologies in IoT. The protocols they have surveyed are RFID, ZigBee, WiFi, and Bluetooth. Furthermore, they presented possible issues that could occur in a practical appliance. The authors have investigated attacks like tampering, packet sniffing and injection, key leakage, bluejacking, bluesnarfing, clandestine scanning and tracking, skimming, and cloning, and exploiting cryptographic weaknesses in general.
Nallusamy et al. [67] have developed a virus propagation and prevention model for heterogeneous IoT networks. The have calculated the propagation in networks as well as human behaviour into the concept.

Concluding Words and Future Research

In this thesis an updated literature review was conducted on the smart home protocols ZigBee, Z-Wave, Thread, BLE, and EnOcean and their respective security features. An extended focus was put on the question of user interaction in the implementation of security features.
For the process of searching, three platforms were chosen as sources: WebofScience, Scopus, and IEEE. Each of these platforms required a tailored search string to produce the best possible number of results. The search strings used produced more than 8,000 results to sift through which was done with the assistance of Zotero. Future research may update the search strings or simplify them according to their needs. Attention must be paid not to make the search strings too restrictive otherwise the number of results might be insufficient for the purpose.
After the platforms have been searched, the results had to be exported as RIS-files to be collected in a Zotero database. This tool helped to analyse the large number of results in an efficient way as all the meta data from the items has been imported by the tool.
To add quality to the review the meta-analysis tool PRISMA 2020 was utilized to properly screen the results. The 27-item checklist of the PRISMA 2020 tool was loosely adapted to create a structure that resembles meta-analyses conducted in other fields of research such as medicine, pharmacology, linguistics, and so on. To produce a qualitative result in this review the final number of database entries in Zotero was narrowed down to 52 items which were then discussed in this thesis.
The results of the literature review are presented in a table, listing author(s), title, purpose, type of source, year, protocols, major themes, attacks/threats mentioned, countermeasures proposed, and user interaction.
The literature review has produced results that suggest the implementation of security features lies mainly in the responsibility of the manufacturers and software developers. Future research could focus on the part of the user and how they can become active in enhancing their overall network and application security (e.g., pay attention to a specific hardware model that already supports security features, this may cost a little more than the legacy model with no security features or weak security). So far, the user takes a more passive role in the security of their smart home network. With this, the question of the role of the users and the developers when it comes to security in the IoT environment has been answered.
At some point in the future another updated literature review may be conducted, and that time, the PRISMA method may be implemented fully. This means that the entire literature review will be written under consideration of the 27-point checklist provided by PRISMA 2020, making sure that the content provided matches the criteria of the checklist.

List of Acronyms

AAA *Authentication Authorization Accounting*
ACLs *Access Control Lists*
AES *Advanced Encryption Standard*
AFH *Adaptive Frequency Hopping spread spectrum*
APS *Application Support*
ASM *Abstract State Machines*
ATT *Attribute Protocol*
BLE Bluetooth Lower Energy
CBC *Cipher Block Chaining*
CCM *Cipher Block Chaining - Message authenticatio Code*
CIA *Confidentiality Integrity Availability*
CoAP *Constrained Application Protocol*
COTS *Commercial-Off-The-Shelf*
CRC *Cycle Redundancy Check*
CSMA/CA *Carrier Sence Multiple Access / Collision Avoidance*
CSRK Connection Signature Resolve Key
CTR *Counter*
DoS *Denial of Service*
DSK Device Specific Key
DTLS 36, *Datagram Transport Layer Security*, *Datagram Transport Layer Security*
DVR *Distance Vector Routing*
ECDH *Elliptic Curve Diffie Hellman*
EUI *Extended Unique Identifier*
FMS *Freight Management System*
FOTA *Firmware-over-the-air*
G2B 14, *Government to Business*
G2C *Government to Citizen*
G2E *Government to Employee*
G2G *Government to Government*
GAP *Generic Addresss Profile*
GATT *Generic Attribute Protocol*
GHz *Gigahertz*
HANs *Home Area Networks*
HDD *Hard Drive Disk*
HMAC *Hash-based Message Authentication Code*
HSNK *High Security Network Key*
I/O *Input-Output*
ICMP *Internet Control Message Protocol*
ID/IP *Intrusion Detection / Intrusion Prevention*
IDS *Intrusioin Detection System*
IoT *Internet of Things*
IRK Identity Resolving Key
ISM *Industrial Scientific Medical*
JR *Joiner Router*
L2CAP *Logical Link Control and Adaptation Protocol*
LK *Link Key*
LTE *Long-Term Evolution*
LTK Long Term Key
MAC *Media Access Control*
ME *Malicious Extensions*
MHz *Megahertz*
MIC *Message Integrity Code*
MLE *Mesh Link Establishment*
MPDU *MAC Protocol Data Unit*
NAK *Negative Acknowledgement*
NFC *Near Field Communication*
NL *Neighbour List*
NVRAM *Non-Volatile Random Access Memory*
NWK *Network*
OOB *Out-of-Band*
OS *Operating System*
PAN *Private Area Network*
PDU *Protocol Data Unit*
PIN Personal Identification Number
PoV *Point-of-View*
PRNG *Pseudo Random Number Generator*
QoS *Quality of Service*
QR Quick Response
RAM *Random Access Memory*
REED *Router Enabled End Device*
RFCOMM Radio Frequency Communication
RFID *Radio Frequency Identification*, *Radio Frequency Identification*
RLC *Rolling Code*
RPA *Resolvable Private Addresssing*
RSSI *Received Signal Strength Indicator*
RT/CR MITM *Real Time/Control Relay Man-in-the-Middle*
RTS/CTS *Request To Send / Clear To Send*
SC *Secure Connection*
SD *Secure Digital Memory Card*
SIG *Special Interest Group*
SM *Security Manager*

SNK *Standard Network Key*
SoA *Service-Oriented Architecture*
SR *Source Routing*
SSD *Solid State Drive*
STK *Short-Term Key*
TC *Trust Center*
TIS *Traveller's Information System*
TK *Temporary Key*
UDP *User Datagram Protocol*
USA *United States of America*
USB *Universal Serial Bus*
V2V *Vehicle-To-Vehicle*
WPAN *Wireless Personal Area Network*
WSN *Wireless Sensor Network*
ZC *ZigBee Controller*
ZDO *Zigbee Device Object*
ZED *ZigBee End Device*
ZR *ZigBee Router*

Bibliograpy

[1] R. Yu, X. Zhang, and M. Zhang, ‘Smart Home Security Analysis System Based on The Internet of Things’, in *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Mar. 2021, pp. 596–599. doi: 10.1109/ICBAIE52039.2021.9389849.

[2] S. Swamy and S. Kota, ‘An Empirical Study on System Level Aspects of Internet of Things (IoT)’, *IEEE ACCESS*, vol. 8, pp. 188082–188134, 2020, doi: 10.1109/ACCESS.2020.3029847.

[3] D. Dragomir, L. Gheorghe, S. Costea, A. Radovici, and IEEE, ‘A Survey on Secure Communication Protocols for IoT Systems (Invited Paper)’, presented at the 2016 INTERNATIONAL WORKSHOP ON SECURE INTERNET OF THINGS (SIOT), 2016, pp. 47–62. doi: 10.1109/SIoT.2016.8.

[4] M. Naglic and A. Souvent, ‘Concept of SmartHome and SmartGrids integration’, in *2013 4th International Youth Conference on Energy (IYCE)*, Jun. 2013, pp. 1–5. doi: 10.1109/IYCE.2013.6604199.

[5] P. Ahmadi, K. Islam, T. Maco, and M. Katam, ‘A survey on internet of things security issues and applications’, in *Proc. - Int. Conf. Comput. Sci. Comput. Intell., CSCI*, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 925–934. doi: 10.1109/CSCI46756.2018.00182.

[6] S. Teerakanok, T. Uehara, and A. Inomata, ‘A secure cloud-centric iot framework for smart device registration’, *J. Info. Process.*, vol. 29, pp. 381–391, 2021, doi: 10.2197/IPSJJIP.29.381.

[7] D. Celebucki, M. Lin, and S. Graham, ‘A Security Evaluation of Popular Internet of Things Protocols for Manufacturers’, presented at the 2018 IEEE INTERNATIONAL CONFERENCE ON CONSUMER ELECTRONICS (ICCE), S. Mohanty, P. Corcoran, H. Li, A. Sengupta, and J. Lee, Eds., 2018.

[8] D.-G. Akestoridis, V. Sekar, and P. Tague, ‘On the Security of Thread Networks: Experimentation with OpenThread-Enabled Devices’, in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, in WiSec ’22. New York, NY, USA: Association for Computing Machinery, Mai 2022, pp. 233–244. doi: 10.1145/3507657.3528544.

[9] P. An, T. Kim, and IEEE, ‘A Study of the Z-Wave Protocol: Implementing Your Own Smart Home Gateway’, presented at the PROCEEDINGS OF 2018 3RD INTERNATIONAL CONFERENCE ON COMPUTER AND COMMUNICATION SYSTEMS (ICCCS), 2018, pp. 411–415.

[10] K. Kim *et al.*, ‘What’s your protocol: Vulnerabilities and security threats related to Z-Wave protocol’, *PERVASIVE AND MOBILE COMPUTING*, vol. 66, Jul. 2020, doi: 10.1016/j.pmcj.2020.101211.

[11] ‘IEEE at a Glance’. https://www.ieee.org/about/at-a-glance.html (accessed Mar. 16, 2023).

[12] G. Kambourakis, C. Kolias, D. Geneiatakis, G. Karopoulos, G. Makrakis, and I. Kounelis, ‘A State-of-the-Art Review on the Security of Mainstream IoT Wireless PAN Protocol Stacks’, *SYMMETRY-BASEL*, vol. 12, no. 4, Apr. 2020, doi: 10.3390/sym12040579.

[13] Y. Tang, H. Lian, L. Li, X. Wang, and X. Yan, ‘A Randomness Detection Method of ZigBee Protocol in a Wireless Sensor Network’, *SENSORS*, vol. 18, no. 11, Nov. 2018, doi: 10.3390/s18113962.

[14] J. Fuller, B. Ramsey, M. Rice, and J. Pecarina, ‘Misuse-based detection of Z-Wave network attacks’, *COMPUTERS & SECURITY*, vol. 64, pp. 44–58, Jan. 2017, doi: 10.1016/j.cose.2016.10.003.

[15] M. Yassein, W. Mardini, T. Almasri, and ASSOC COMP MACHINERY, ‘Evaluation of security regarding Z-Wave wireless protocol’, presented at the ICEMIS’18: PROCEEDINGS OF THE

FOURTH INTERNATIONAL CONFERENCE ON ENGINEERING AND MIS, 2018. doi: 10.1145/3234698.3234730.
[16] C. Badenhop, S. Graham, B. Ramsey, B. Mullins, and L. Mailloux, 'The Z-Wave routing protocol and its security implications', *COMPUTERS & SECURITY*, vol. 68, pp. 112–129, Jul. 2017, doi: 10.1016/j.cose.2017.04.004.
[17] A. Lonzetta, P. Cope, J. Campbell, B. Mohd, and T. Hayajneh, 'Security Vulnerabilities in Bluetooth Technology as Used in IoT', *JOURNAL OF SENSOR AND ACTUATOR NETWORKS*, vol. 7, no. 3, Sep. 2018, doi: 10.3390/jsan7030028.
[18] P. Sivakumaran, J. Blasco, and USENIX Assoc, 'A Study of the Feasibility of Co-located App Attacks against BLE and a Large-Scale Analysis of the Current Application-Layer Security Landscape', presented at the PROCEEDINGS OF THE 28TH USENIX SECURITY SYMPOSIUM, 2019, pp. 1–18.
[19] K. Fawaz, K. Kim, K. Shin, and USENIX Assoc, 'Protecting Privacy of BLE Device Users', presented at the PROCEEDINGS OF THE 25TH USENIX SECURITY SYMPOSIUM, 2016, pp. 1205–1221.
[20] A. Barua, M. Al Alamin, M. Hossain, and E. Hossain, 'Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey', *IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY*, vol. 3, pp. 251–281, 2022, doi: 10.1109/OJCOMS.2022.3149732.
[21] R. Cayre *et al.*, 'WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips', presented at the 51ST ANNUAL IEEE/IFIP INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS (DSN 2021), 2021, pp. 376–387. doi: 10.1109/DSN48987.2021.00049.
[22] I. Unwala, Z. Taqvi, J. Lu, and IEEE, 'IoT Security : ZWave and Thread', presented at the 2018 IEEE GREEN TECHNOLOGIES CONFERENCE (GREENTECH), 2018, pp. 176–182. doi: 10.1109/GreenTech.2018.00040.
[23] T. Choudhury, A. Gupta, S. Pradhan, P. Kumar, and Y. S. Rathore, 'Privacy and Security of Cloud-Based Internet of Things (IoT)', in *Proc. - Int. Conf. Comput. Intell. Networks, CINE*, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 40–45. doi: 10.1109/CINE.2017.28.
[24] 'CWE - 2022 CWE Top 25 Most Dangerous Software Weaknesses', *2022 CWE Top 25 Most Dangerous Software Weaknesses*, Mar. 10, 2023. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html (accessed Mar. 10, 2023).
[25] M. A. Bin Karnain and Z. Bin Zakaria, 'A review on ZigBee security enhancement in smart home environment', in *IEEE Int. Conf. Inf. Sci. Secur., ICISS*, Institute of Electrical and Electronics Engineers Inc., 2016. doi: 10.1109/ICISSEC.2015.7370969.
[26] D. York, 'CHAPTER 3 - Eavesdropping and Modification', in *Seven Deadliest Unified Communications Attacks*, D. York, Ed., Boston: Syngress, 2010, pp. 41–69. doi: 10.1016/B978-1-59749-547-9.00003-X.
[27] Amiruddin, A. Ratna, R. Sari, and IEEE, 'A Testbed Implementation of Secure and Lightweight Privacy Preservation Mechanism Using Scrambled Fibonacci and XOR for ZigBee', presented at the TENCON 2017 - 2017 IEEE REGION 10 CONFERENCE, 2017, pp. 863–868.
[28] 'What is a denial of service attack (DoS) ?', *Palo Alto Networks*. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos (accessed Mar. 11, 2023).
[29] vardaanpruthi, 'Wormhole Attack in Wireless Sensor Networks', *GeeksforGeeks*, Jan. 08, 2020. https://www.geeksforgeeks.org/wormhole-attack-in-wireless-sensor-networks/ (accessed Mar. 11, 2023).
[30] 'Sinkhole Attack in Wireless Sensor Networks', *GeeksforGeeks*, Feb. 27, 2020. https://www.geeksforgeeks.org/sinkhole-attack-in-wireless-sensor-networks/ (accessed Mar. 11, 2023).

[31] ‘Attacks in the IoT’, *Ebrary*. https://ebrary.net/180673/computer_science/attacks (accessed Mar. 11, 2023).
[32] ‘What is MITM (Man in the Middle) Attack | Imperva’, *Learning Center*. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (accessed Mar. 11, 2023).
[33] ‘Kali Linux - Sniffing and Spoofing’, *GeeksforGeeks*, Sep. 23, 2020. https://www.geeksforgeeks.org/kali-linux-sniffing-and-spoofing/ (accessed Mar. 11, 2023).
[34] ‘Replay Attack’, *GeeksforGeeks*, Jun. 18, 2020. https://www.geeksforgeeks.org/replay-attack/ (accessed Mar. 11, 2023).
[35] K. Lounis and M. Zulkernine, ‘Attacks and Defenses in Short-Range Wireless Technologies for IoT’, *IEEE ACCESS*, vol. 8, pp. 88892–88932, 2020, doi: 10.1109/ACCESS.2020.2993553.
[36] M. Grabovica, D. Pezer, S. Popic, V. Knezevic, and IEEE, ‘Provided security measures of enabling technologies in Internet of Things (IoT): A survey’, presented at the 2016 ZOOMING INNOVATION IN CONSUMER ELECTRONICS INTERNATIONAL CONFERENCE (ZINC), 2016, pp. 28–31. doi: 10.1109/ZINC.2016.7513647.
[37] J. Tournier, F. Lesueur, F. Le Mouel, L. Guyon, and H. Ben-Hassine, ‘A survey of IoT protocols and their security issues through the lens of a generic IoT stack’, *INTERNET OF THINGS*, vol. 16, Dec. 2021, doi: 10.1016/j.iot.2020.100264.
[38] K. Narayanan, ‘Addressing the challenges facing IoT adoption’, *Microwave J*, vol. 60, no. 1, pp. 110–118, 2017.
[39] G. Varshney, M. Misra, and P. Atrey, ‘A New Secure Authentication Scheme for Web Login Using BLE Smart Devices’, presented at the PROCEEDINGS OF 2017 11TH IEEE INTERNATIONAL CONFERENCE ON ANTI-COUNTERFEITING, SECURITY, AND IDENTIFICATION (ASID), J. Zhou, D. Guo, and J. Dong, Eds., 2017, pp. 95–98.
[40] S. Sarkar, H. Liu, E. Jovanov, and IEEE, ‘A Robust Algorithm for Sniffing BLE Long-Lived Connections in Real-time’, presented at the 2019 IEEE GLOBAL COMMUNICATIONS CONFERENCE (GLOBECOM), 2019.
[41] S. Sevier, A. Tekeoglu, and IEEE, ‘Analyzing the Security of Bluetooth Low Energy’, presented at the 2019 INTERNATIONAL CONFERENCE ON ELECTRONICS, INFORMATION, AND COMMUNICATION (ICEIC), 2019, pp. 568–572.
[42] S. Pallavi, V. Narayanan, and IEEE, ‘An Overview of Practical Attacks on BLE Based IOT Devices and Their Security’, presented at the 2019 5TH INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING & COMMUNICATION SYSTEMS (ICACCS), 2019, pp. 694–698.
[43] Md. J. H. Biddut, N. Islam, R. S. Sultana, A. Sarker, and M. M. Rahman, ‘A new approach of ZigBee MAC layer design based on security enhancement’, in *IEEE Int. Conf. Telecommun. Photonics, ICTP*, Institute of Electrical and Electronics Engineers Inc., 2016. doi: 10.1109/ICTP.2015.7427934.
[44] P. Morgner, S. Mattejat, Z. Benenson, C. Muller, F. Armknecht, and ACM, ‘Insecure to the Touch: Attacking ZigBee 3.0 via Touchlink Commissioning’, presented at the PROCEEDINGS OF THE 10TH ACM CONFERENCE ON SECURITY AND PRIVACY IN WIRELESS AND MOBILE NETWORKS (WISEC 2017), 2017, pp. 230–240. doi: 10.1145/3098243.3098254.
[45] B. Fan and IEEE, ‘Analysis on the Security Architecture of ZigBee Based on IEEE 802.15.4’, presented at the 2017 IEEE 13TH INTERNATIONAL SYMPOSIUM ON AUTONOMOUS DECENTRALIZED SYSTEMS (ISADS 2017), 2017, pp. 241–246. doi: 10.1109/ISADS.2017.23.
[46] X. Cao, D. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, ‘Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks’, *IEEE INTERNET OF THINGS JOURNAL*, vol. 3, no. 5, pp. 816–829, Oct. 2016, doi: 10.1109/JIOT.2016.2516102.
[47] L. Li, P. Podder, and E. Hoque, ‘A formal security analysis of ZigBee (1.0 and 3.0)’, in *ACM Int. Conf. Proc. Ser.*, Association for Computing Machinery, 2020, pp. 101–111. doi: 10.1145/3384217.3385617.

[48] M. Lilli, C. Braghin, and E. Riccobene, ‘Formal Proof of a Vulnerability in Z-Wave IoT Protocol’, presented at the SECRYPT 2021: PROCEEDINGS OF THE 18TH INTERNATIONAL CONFERENCE ON SECURITY AND CRYPTOGRAPHY, S. DiVimercati and P. Samarati, Eds., 2021, pp. 198–209. doi: 10.5220/0010553301980209.
[49] S. Marksteiner, V. Jimenez, H. Vallant, and H. Zeiner, ‘An Overview of Wireless IoT Protocol Security in the Smart Home Domain’, presented at the 2017 JOINT 13TH CTTE AND 10TH CMI CONFERENCE ON INTERNET OF THINGS - BUSINESS MODELS, USERS, AND NETWORKS, M. Falch, Ed., 2017.
[50] Y. Liu, K. Hassan, M. Karlsson, Z. Pang, and S. Gong, ‘A Data-Centric Internet of Things Framework Based on Azure Cloud’, *IEEE ACCESS*, vol. 7, pp. 53839–53858, 2019, doi: 10.1109/ACCESS.2019.2913224.
[51] D. Antonioli, N. Tippenhauer, and K. Rasmussen, ‘Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy’, *ACM TRANSACTIONS ON PRIVACY AND SECURITY*, vol. 23, no. 3, Jul. 2020, doi: 10.1145/3394497.
[52] P. Sivakumaran, J. Alis, and ACM, ‘A Low Energy Profile: Analysing Characteristic Security on BLE Peripherals’, presented at the PROCEEDINGS OF THE EIGHTH ACM CONFERENCE ON DATA AND APPLICATION SECURITY AND PRIVACY (CODASPY’18), 2018, pp. 152–154. doi: 10.1145/3176258.3176945.
[53] K. Campos-Cruz, C. Mancillas-Lopez, B. Ovilla-Martinez, and IEEE, ‘A Lightweight Security Protocol for Beacons BLE’, presented at the 2021 18TH INTERNATIONAL CONFERENCE ON ELECTRICAL ENGINEERING, COMPUTING SCIENCE AND AUTOMATIC CONTROL (CCE 2021), 2021. doi: 10.1109/CCE53527.2021.9633037.
[54] D. J. Bernstein, ‘Curve25519: new Diffie-Hellman speed records’, presented at the International Workshop on Public Key Cryptography, Springer, 2006, pp. 207–228.
[55] S. Cha, M. Chuang, K. Yeh, Z. Huang, and C. Su, ‘A User-Friendly Privacy Framework for Users to Achieve Consents With Near by BLE Devices’, *IEEE ACCESS*, vol. 6, pp. 20779–20787, 2018, doi: 10.1109/ACCESS.2018.2820716.
[56] Z. Guo, I. Harris, Y. Jiang, L. Tsaur, and IEEE, ‘An Efficient Approach to Prevent Battery Exhaustion Attack on BLE-based Mesh Networks’, presented at the 2017 INTERNATIONAL CONFERENCE ON COMPUTING, NETWORKING AND COMMUNICATIONS (ICNC), 2016, pp. 1–5.
[57] M. J. Page *et al.*, ‘The PRISMA 2020 statement: an updated guideline for reporting systematic reviews’, *International journal of surgery*, vol. 88, p. 105906, 2021.
[58] ‘Web of Science Core Collection Help’. https://images.webofknowledge.com/images/help/WOS/hs_search_operators.html (accessed Mar. 27, 2023).
[59] S. Hussain, S. Mehnaz, S. Nirjon, E. Bertino, and ACM, ‘Seamless and Secure Bluetooth LE Connection Migration’, presented at the PROCEEDINGS OF THE SEVENTH ACM CONFERENCE ON DATA AND APPLICATION SECURITY AND PRIVACY (CODASPY’17), 2017, pp. 147–149. doi: 10.1145/3029806.3029840.
[60] M. C. Francisco, S. Eisa, and M. L. Pardal, ‘Secure protocol buffers for Bluetooth Low-Energy communication with wearable devices’, in *IEEE Int. Symp. Netw. Comput. Appl., NCA*, Andreolini M., Marchetti M., and Avresky D.R., Eds., Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/NCA53618.2021.9685944.
[61] E. A. Asonye, I. Anwuna, and S. M. Musa, ‘Securing ZigBee IoT Network against HULK Distributed Denial of Service Attack’, in *HONET - IEEE Int. Conf. Smart Commun.: Improv. Qual. Life using ICT, IoT AI*, Institute of Electrical and Electronics Engineers Inc., 2020, pp. 156–162. doi: 10.1109/HONET50430.2020.9322808.
[62] H. Pirayesh, P. Sangdeh, and H. Zeng, ‘Securing ZigBee Communications Against Constant Jamming Attack Using Neural Network’, *IEEE INTERNET OF THINGS JOURNAL*, vol. 8, no. 6, pp. 4957–4968, Mar. 2021, doi: 10.1109/JIOT.2020.3034128.

[63] D.-G. Akestoridis, M. Harishankar, M. Weber, and P. Tague, ‘Zigator: Analyzing the security of zigbee-enabled smart homes’, in *WiSec - Proc. ACM Conf. Secur. Priv. Wirel. Mob. Networks*, Association for Computing Machinery, 2020, pp. 77–88. doi: 10.1145/3395351.3399363.
[64] L. Babun *et al.*, ‘Z-IOT: Passive Device-class Fingerprinting of ZigBee and Z-Wave IoT Devices’, presented at the ICC 2020 - 2020 IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC), 2020.
[65] F. Farha, H. Ning, S. Yang, J. Xu, W. Zhang, and K. Choo, ‘Timestamp Scheme to Mitigate Replay Attacks in Secure ZigBee Networks’, *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 21, no. 1, pp. 342–351, Jan. 2022, doi: 10.1109/TMC.2020.3006905.
[66] M. Ren, X. Ren, H. Feng, J. Ming, and Y. Lei, ‘Z-Fuzzer: Device-agnostic fuzzing of Zigbee protocol implementation’, in *WiSec - Proc. ACM Conf. Secur. Priv. Wirel. Mob. Networks*, Association for Computing Machinery, Inc, 2021, pp. 347–358. doi: 10.1145/3448300.3468296.
[67] T. Nallusamy, R. Ravi, and G. Sathiyaprabhu, ‘Virus propagation in heterogeneous Zigbee networks with human behaviours’, in *Proc. Int. Conf. Intell. Syst. Control, ISCO*, Smys S., Ed., Institute of Electrical and Electronics Engineers Inc., 2016. doi: 10.1109/ISCO.2016.7726891.