Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Bakalářská práce

Porovnání bezdrátových komunikačních technologií ZigBee a Z-Wave

Vedoucí práce: Ing. Zdeněk Votruba, Ph.D.
Autor práce: Jan Čepera

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Čepera

Zemědělské inženýrství

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Porovnání bezdrátových komunikačních technologií ZigBee a Z-Wave

Název anglicky

Comparison of ZigBee and Z-Wave wireless communication technologies

---

Cíle práce

Cílem práce je analýza informací o moderních bezdrátových komunikačních technologiích ZigBee a Z-Wave. Bude provedeno porovnání těchto technologií podle vybraných kritérií.

Metodika

1. Úvod
2. Cíl práce a metodika
3. Popis bezdrátové komunikační technologie ZigBee
4. Popis bezdrátové komunikační technologie Z-Wave
5. Porovnání bezdrátových komunikačních technologií ZigBee a Z-Wave
6. Oblasti využití jednotlivých technologií
7. Vyhodnocení výhod a nevýhod použití technologií ZigBee a Z-Wave
8. Závěr a doporučení

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

IoT, počítačová komunikace, počítačové protokoly, aplikace

Doporučené zdroje informací

BURIAN, P: Internet inteligentních aktivit, Grada 2014, e-kniha
Internetové zdroje, např. https://www.e15.cz/magazin/prumysl-prochazi-zmenou-jako-nikdy-predtim-rika-autor-knihy-o-internetu-veci-1333263
James F. Kurose, Keith W. Ross: Počítačové sítě, CPress, 2014, 3. vydání
Maciej Kranz: Budování internetu věcí, New York Times, 2017

Předběžný termín obhajoby

2019/2020 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 7. 1. 2019

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 15. 2. 2019

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 07. 04. 2020

Čestné prohlášení

„Prohlašuji, že jsem bakalářskou práci na téma „Porovnání bezdrátových komunikačních technologií ZigBee a Z-Wave“ vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

V Praze dne ……..……

Jan Čepera

Poděkování

Rád bych touto cestou poděkoval panu Ing. Zdeňku Votrubovi, Ph.D. za pomoc při vybírání tématu mé bakalářské práce a za to, že mi umožnil pracovat pod jeho odborným vedením. Dále bych rád poděkoval Ing. Pavlíně Čeperové, Ing. Jiřímu Čeperovi a Barboře Pražákové za velkou oporu a cenné rady při psaní této práce.

Abstrakt: Cílem této bakalářské práce bylo porovnání bezdrátových komunikačních technologií ZigBee a Z-Wave, které jsou založeny na standardu IEEE 802.15.4. V kapitole „Bezdrátový přenos dat“ jsou stručně popsány způsoby, jakými lze data bezdrátově přenášet. V kapitole „Bezdrátová síť PAN IEEE 802.15.4“ je stručně popsán standard IEEE 802.15.4. Dále se tato kapitola zabývá prvky a topologií sítě krátkého dosahu. V následujících dvou kapitolách jsou vysvětleny jednotlivé komunikační technologie ZigBee a Z-Wave. Dále je provedeno vzájemné porovnání a vyhodnocení výhod a nevýhod těchto bezdrátových komunikačních technologií na základě několika vybraných parametrů. Na závěr je provedeno vyhodnocení těchto komunikačních technologií a je nastíněno, jakým směrem by se mohl ubírat jejich vývoj.

Klíčová slova: IoT, počítačová komunikace, počítačové protokoly, aplikace

Comparison of ZigBee and Z-Wave wireless communication technologies

Summary: The object of this thesis is comparing wireless communication technologies ZigBee and Z-Wave. These technologies are working on IEEE 802.15.4. standard. In the “Wireless data transmission” chapter are briefly described ways of wireless data transmission. In the “Wireless net PAN IEEE 802.15.4.” is a brief description of the IEEE 802.15.4. standard with elements and topology of the small range net. In two following chapters is described each communication technology ZigBee and Z-Wave. Next there is a mutual comparison and evaluation of advantages and disadvantages of said communication technologies based on chosen parameters. In conclusion is done final evaluation of said communication technologies and also there is a prediction on their future development.

Keywords: IoT, computer communication, computer protocols, application

Obsah

1 Úvod

S postupem času je lidstvo čím dál tím více obklopeno automatizovanými systémy, které značně usnadňují práci – jak v průmyslovém odvětví, tak i v domácí automatizaci. A právě domácí automatizace se stává trendem dnešní uspěchané doby. Na trhu je kromě velkého množství výrobců elektronických zařízení k dispozici i značné množství komunikačních technologií, které jsou využívány pro automatizaci v domácnosti. Například protokoly LoRaWAN, Cellular, AMQP, dokonce i celosvětově známé Bluetooth využívající komunikační standard IEEE 802.15.4. Neuplynula však příliš dlouhá doba od chvíle, kdy se na trhu začaly objevovat komunikačních technologie s názvy ZigBee a Z-Wave, které také tento standard využívají.

Automatizace domácnosti není v současné době nic neobvyklého. Už desítky let se do moderních budov instalují prvky poplachových zabezpečovacích a tísňových systémů, elektronické zámky na dálkové ovládání, centrální řízení vzduchotechniky, světel apod. Nároky uživatelů těchto „vylepšení“ se však neustále zvyšovaly a uživatelé se nespokojili s možnostmi, jak tyto systémy ovládat. Ideálně potřebovali jediné zařízení, odkud by mohli všechny tyto systémy ovládat najednou. A právě tyto možnosti přináší bezdrátové komunikační technologie ZigBee a Z-Wave, kterými se tato práce zabývá.

V prvních kapitolách této práce je stručně vysvětlena problematika možností bezdrátového přenosu dat a dále je popsán komunikační standard IEEE 802.15.4, který s řešenými technologiemi bezprostředně souvisí.

Stále oblíbenější bezdrátovou technologií se stává ZigBee a to nejen v domácí automatizaci. A právě ZigBee je věnována celá kapitola, kde se čtenář dozví o její stručné historii, o ZigBee Alianci a následně bude seznámen se samotným protokolem z technologického hlediska. Následující kapitola pak představuje konkurenční technologii Z-Wave. Taktéž odkrývá náhled do její minulosti a seznamuje čtenáře s technologickou stránkou protokolu.

V závěrečné části této práce je provedeno porovnání výše uvedených bezdrátových komunikačních technologií podle fyzikálních, aplikačních a zabezpečovacích rozdílů.

2 Cíl práce

Cílem této bakalářské práce je analýza informací o neustále se vyvíjejících bezdrátových komunikačních technologií ZigBee a Z-Wave. Kromě analýzy informací si práce klade za cíl provést porovnání těchto technologií na základě fyzikálních, aplikačních a bezpečnostních rozdílů a seznámit tak čtenáře s případnými výhodami či nevýhodami konkrétní technologie. V neposlední řadě se tato práce zabývá problematikou bezdrátového přenosu a teorií standardu IEEE 802.15.4.

Tato práce by se dala použít jako určitý návod pro zákazníky, kteří vybírají mezi těmito technologiemi a chtějí zjistit, která je pro jejich účel vhodnější.

3 Metodika

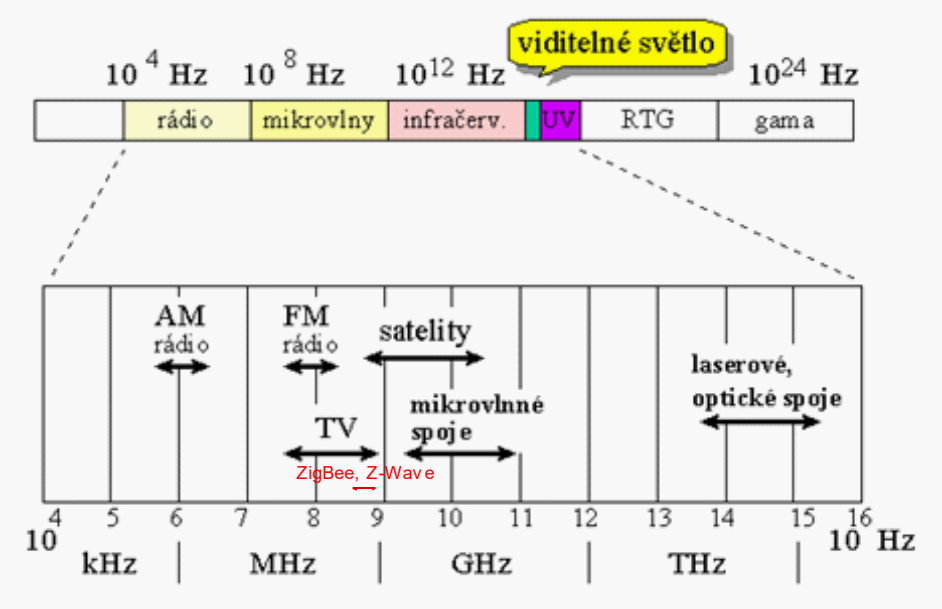
Práce je rozdělena do několika částí. První část se zabývá problematikou bezdrátového přenosu a popisuje možné způsoby přenosu dat. Druhá část práce se ve stručnosti zabývá standardem IEEE 802.15.4 kde popisuje prvky sítě krátkého dosahu a topologii. Dvě následující části práce se zabývají analýzou informací o bezdrátových komunikačních technologiích ZigBee a Z-Wave. Zde je stručně popsána historie obou technologií a jsou vysvětleny principy fungování. Poslední kapitola se potom zabývá porovnáním těchto technologií na základě fyzikálních a aplikačních rozdílů.

4 Bezdrátový přenos dat

Jednou z nevýhod drátových přenosů dat je nutnost instalace kabelů, která mnohdy není z různých důvodů vůbec možná. Řešením pak mohou být různé bezdrátové přenosové technologie, ve kterých se pro přenos dat využívá nejčastěji elektromagnetických vln nebo světelného záření. Vzdálenost, kterou je možné bezdrátovými technologiemi pokrýt, závisí na konkrétní instalaci. Může být v řádech několika metrů až desítkách či stovkách kilometrů, a to při zachování vysoké přenosové rychlosti, která je v dnešní době již srovnatelná s rychlostmi u drátových přenosů. [1] [2]

4.1 Způsoby přenosu dat

Jak již bylo řečeno v úvodu do této kapitoly, v bezdrátovém přenosu se nejčastěji využívá elektromagnetických vln. V této podkapitole budou popsána jednotlivá frekvenční pásma v elektromagnetickém spektru, která je možná využít pro přenosy – konkrétně rádiová, mikrovlnná a infračervená část spektra. Vyšší části spektra jsou pro přenosy teoreticky možné, ale jejich použití je zdraví škodlivé a jejich modulování je obtížné. [2] Jednotlivé části spektra jsou znázorněny na obrázku 1.



Obrázek 1 Elektromagnetické spektrum [3] (upraveno autorem)

4.2 Rádiové přenosy

V této oblasti spektra musí být silný centrální dohled nad přidělováním frekvencí a jejich využitím díky relativně velkému dosahu rádiových vln a nutnosti koordinace konkrétních frekvenčních pásem. Díky této koordinaci je zamezeno nežádoucímu prolínání rádiových přenosů. Dosah a prostupnost rádiových frekvencí skrze různé překážky závisí na konkrétní frekvenci. Při využití nižších frekvencí vlny sice snadněji pronikají překážkami, ale mají krátký dosah. U vyšších frekvencí se vlny šíří více přímočaře a mají tendenci se od překážek odrážet. Nevýhodou rádiových vln je malá šířka přenosového pásma. Z tohoto důvodu není vhodné používání tohoto typu přenosu na objemná data. Jako další nevýhodu lze možno brát i ovlivňování šíření povětrnostními podmínkami. Za výhodu lze považovat snadné generování i přijímání elektromagnetických vln v této části spektra. Další výhodou je všesměrové šíření rádiových vln, takže není nutné anténu vysílače a přijímače speciálně směrovat. [2]

4.3 Kmitočtová pásma

Rádiové spektrum je podle ČTU rozděleno na devět pásem (viz Tabulka 1), která jsou značena celými čísly od 4 do 12. Jednotkou kmitočtu je hertz (Hz) a je vyjadřován následovně:

- v kilohertzích (kHz) do 3000 kHz včetně,
- v megahertzích (MHz) od 3 MHz do 3000 MHz včetně,
- v gigahertzích (GHz) od 3 GHz do 3000 GHz včetně [4]

Číslo pásma	Symbol	Rozsah kmitočtů	Název pásem
4	VLF	3 až 30 kHz	myriametrové
5	LF	30 až 300 kHz	kilometrové
6	MF	300 až 3000 kHz	hektometrové
7	HF	3 až 30 MHz	dekametrová
8	VHF	30 až 300 MHz	metrové
9	UHF	300 až 3000 MHz	decimetrové
10	SHF	3 až 30 GHz	centimetrové
11	EHF	30 až 300 GHz	milimetrové
12		300 až 3000 GHz	decimilimetrové

Tabulka 1 Pásma rádiového spektra (vlastní, dle dat z [4])

4.4 Mikrovlnné přenosy

Elektromagnetické vlny v pásmu nad 100 MHz se šíří velmi přímočaře a je tedy možné soustředit energii do úzce směrovaného paprsku. Úzce směrovaný paprsek snižuje problémy se vzájemným ovlivňováním a přeslechem přenosů. Přenos pomocí mikrovln lze realizovat na poměrně dlouhé vzdálenosti. Ty jsou však v praxi limitovány terénními překážkami, které jsou těžce prostupné. Proto se využívá retranslačních stanic, umístěných ve vhodných vzdálenostech od sebe, které zvyšují dosah přenosu. [2]

Přenosy v této části spektra v praxi nejsou řešeny pouze jako úzce směrované, použití tedy není omezeno přímým dohledem vysílače a přijímače. Antény základnových stanic jsou řešeny tak, aby pokryly celé své okolí nebo jeho určitou část a umožnily tak opačným komunikujícím stranám pohyb v rámci pokrytého území. Na tomto principu funguje například komunikace GSM. Komunikace tohoto typu má omezený počet přenosových kanálů, které jsou uživatelům dynamicky přidělovány. Díky tomu nejsou přenosy vzájemně rušeny. [2]

4.5 Přenosy v infračervené části spektra

K přenosu v infračervené části spektra je zapotřebí vysílač a přijímač infračerveného záření převádějící elektrický signál na optické záření a naopak. Aby byl zajištěn bezpečný přenos dat na větší vzdálenost, je nutno použít vysílací diodu s velkým výkonem. Na straně příjemce je nutno zajistit použití diody s vysokou citlivostí na záření v daném pásmu. Při použití v praxi je nutné omezit vliv ostatních zdrojů záření. Proto se přijímací dioda zalévá do vhodně tvarovaného pouzdra, které slouží jako optický filtr, čímž dochází k selekci přijímaného pásma před vstupem na přijímací diodu. [5]

Výhodou tohoto typu přenosu je nenáročnost realizace a její nízká cena. Vzhledem k omezenému dosahu není použití omezeno žádnou licencí. Velkou nevýhodou je způsob šíření vln. Ty nemají schopnost procházet překážkami, a tak je použití omezeno na velmi krátkou vzdálenost. [2]

5 Bezdrátová síť PAN IEEE 802.15.4

Standard IEEE 802.15.4 popisuje rádiovou komunikaci pro sítě krátkého dosahu. Norma zajišťuje vysokou spolehlivost přenosu i při jednoduché implementaci s ohledem na omezení spotřeby koncových zařízení. [6]

Cílem pro vytvoření této normy bylo poskytnutí takové technologie, která bude vhodná k implementování tam, kde se současné protokoly jeví předimenzované, složité a v neposlední řadě drahé. Architektura komunikačního modelu tohoto standardu je tvořena dvěma vrstvami – nižší fyzická vrstva a vrstva přístupu k médiu. Vrstva řízení přístupu k médiu zodpovídá za připojení a odpojení uzlu od sítě. Zároveň může poskytovat mechanismus nadrámců společně se synchronizačními rámci a garantovanými časovými úseky pro přenosy s vyšší prioritou. Bezlicenční frekvenční pásma 915 MHz či 2,4 GHz a licencované pásmo 868 MHz umožňují souhrnné použití sítě se zřetelem na omezení místních telekomunikačních prostředků. Ve frekvenčních pásmech 868 MHz a 915 MHz jsou data přenášena technikou přímého rozprostřeného spektra při použití binární fázové modulace. V pásmu 2,4 GHz je pro přenos využito kvadraturní fázové modulace. [7]

5.1 Prvky PAN

V síti se společně vyskytují dva druhy zařízení, které se liší řadou primitiv služeb.

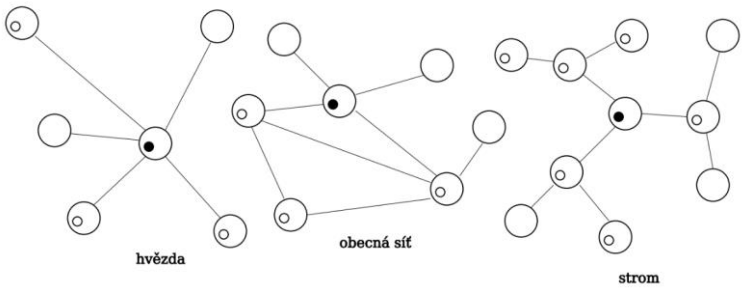
- Plně funkční zařízení (FFD) – Zohledňuje veškerá primitiva služeb, která jsou standardem IEEE 802.15.4 definována. Toto zařízení je schopno zastávat funkci koordinátora PAN, směrovače i koncového zařízení. [7] (viz. Kapitola 5.2)
- Zařízení s omezenou funkčností (RFD) – Toto zařízení pokrývá základní primitiva služeb a lze ho využít jedině jako zařízení koncové. Z hlediska topologie se jedná o koncové uzly větví. Není možné je vzájemně spojit a ani nemohou dále posílat přijatá data. Proto se v praxi používají pro jednoduché úkony nevyžadující časté a objemné přenosy – například pro senzory a tlačítka. Komunikace tohoto druhu zařízení je omezena na odesílání informací koordinátoru v daných časových intervalech, čímž lze znatelně snížit spotřebu energie. Mohou být nahrazena plně funkčními zařízeními.

Každá síť musí obsahovat právě jednoho koordinátora, přičemž počet dalších zařízení je volitelný a závisí na adresním rozsahu. [7]

5.2 Topologie

IEEE 802.15.4 podporuje 3 typy topologií bezdrátové sítě osobního dosahu. Pří výběru topologie je nutno vzít v úvahu, které uzly jsou napájeny z baterie, které ze sítě, očekáváná životnost baterie, náklady na realizaci apod. [8]

- **Hvězda** – V této topologii se nachází jeden centrální uzel v pozici koordinátora. Každé ze zařízení (RFD, FFD) odesílá data centrálnímu uzlu. Tento uzel pak data doručí příjemci. Použití této topologie není ničím omezeno, ale je doporučována pro sítě s velmi malým rozsahem a napájeným centrálním uzlem přímo ze sítě. Tento druh topologie není možné využít v senzorických sítích z toho důvodu, že senzorické sítě využívají ve většině případů bateriové napájení, které není schopné dodržet životnost udávanou normou. [7]
- **Obecná síť (mesh)** – V této topologii se nachází jeden uzel zastupující roli koordinátora sítě. Každý uzel má možnost navázat spojení se všemi okolními uzly v jeho rozsahu. Oproti hvězdové topologii je tato topologie složitější. Uzlové spoje jsou zcela náhodné a trasa, která vede přes několik účastníků se může změnit. U této topologie je tedy možné vytvářet pokročilejší a užitečnější sítě. [7]
- **Strom** – Tato topologie je speciálním případem obecné sítě. Koordinátor sítě představuje centrální prvek. Dalšími prvky sítě jsou koncový uzel a koordinátor oddílu. Koordinátor oddílu je spojen s jedním nadřazeným uzlem a s alespoň s jedním podřízeným uzlem. Nadřízený uzel je buď koordinátor sítě či koordinátor oddílu. Podřízeným uzlem může být koncové zařízení nebo koordinátor oddílu. [7]



Obrázek 2 Topologie standardu 802.15.4 [7]

6 Komunikační technologie ZigBee

Název této technologie pochází z procesu existujícího v přírodě. Když včely létají zpět do svého úlu, provádějí takzvaný kývavý tanec, na který slovní spojení ZigBee odkazuje. Sítě ZigBee jsou založeny na standardu IEEE 802.15.4 pro WPAN, tedy pro sítě s malým dosahem. Jsou navrženy pro sítě, které využívají inteligentní snímače s malým vysílacím výkonem, schopné pokrýt rozsáhlé oblasti. Síť ZigBee lze použít především na místech, kde se klade důraz na nízkou cenu – sbírání dat ze senzorů, měření ve zdravotnictví, automatizace zařízení budov apod. [8] [9] [10]

Obrázek 3: Logo ZigBee [11]

6.1 Historie

Jako první zde byly sítě Bluetooth a Wi-Fi, které byly prohlášeny za standardy v D2D a HDR doménách, jako je například streamování videa a audia. Nebyly ale vhodné pro některé aplikace, a tak si mnoho inženýrů uvědomilo, že je potřeba realizovat novou ad–hoc digitální rádiovou síť. Díky této potřebě začaly v roce 1998 vznikat první sítě ve stylu ZigBee. Standard IEEE 802.15.4, na kterém je tato komunikační technologie založena, byl dokončen v květnu 2003. V této době byli Philips Semiconductors (nyní NXP Semiconductors) hlavním podporovatelem této sítě, ale svou investici zastavili. Avšak společnost Philips Lighting pokračovala v účasti společnosti Philips na projektu. [8]

6.1.1 Verze ZigBee

S postupem času se verze ZigBee neustále vyvíjely a zdokonalovaly. První specifikace ZigBee byly ratifikovány v prosinci 2004. [8]

- **ZigBee 2004 Specificiation** – Tato verze byla dokončena v roce 2004 a následně vydána v roce 2005. [8]

- **ZigBee 2006 Specificiation** – Tato verze byla dokončena a vydána v roce 2006. [8]

- **ZigBee PRO** – Tato vylepšená verze byla dokončena a vydána v posledním čtvrtletí roku 2007. [8]

- **ZigBee 3.0** -Verze 3.0 je založena na ZigBee PRO. Zachovává všechny předchozí funkce, ale sjednocuje profily aplikací a umožňuje všem zařízením se bezdrátově připojit ke stejné síti – zde je možné propojení různých zařízení od různých výrobců při zachování vzájemné komunikace jednotlivých zařízení. [8]

6.1.2 ZigBee Alliance

ZigBee Alliance je otevřené neziskové sdružení řídící vývoj inovativních standardů ZigBee, které ve své podstatě přinášejí větší svobodu a flexibilitu každodenního života. Podporuje celosvětové přijetí komunikační technologie ZigBee jako předního bezdrátového síťového, snímacího a kontrolního standardu pro použití ve spotřebitelských, obchodních a průmyslových oblastech, a to především napříč výkonnými technologickými odvětvími. [12]

ZigBee Alliance poskytuje šetrné, nízkoenergetické a otevřené globální bezdrátové standardy zaměřené na monitorování, ovládání a senzorové aplikace s velkým množstvím inteligentních funkcí určených k zajištění komunikace zařízení v různých prostředích, a to po celém světě. [12]

Členové sdružení pocházejí z různých organizací z celého světa. Mezi nejznámější členy patří například Google, Apple, Ikea, Legrand, Assa Abloy aj. [13]

6.2 Technologická zařízení

V typické infrastruktuře ZigBee zapojení se vyskytují tři druhy zařízení, které společně vytvářejí fungující ZigBee síť. Tyto typy zařízení jsou popsány v následujících podkapitolách.

6.2.1 Koordinátor

Koordinátor v ZigBee infrastruktuře představuje uzel, který musí být minimálně jeden, jelikož je jediným zařízením v síti, které ji může spustit. Je zodpovědný za bezpečnost celé sítě, výběr kanálu, ID PAN a profil zásobníku. Zároveň může komunikovat s ostatními zařízeními a směrovat jednotlivé pakety. Pro zajištění správného výběru kanálu a nepoužitého ID PAN koordinátor vykonává celou řadu skenů, a to pro to, aby zjistil jakoukoliv aktivitu na různých kanálech a objevil tak blízké PAN v provozu. Koordinátor provede skenování energie na více frekvencích, aby detekoval energetické hladiny na každém kanálu. Následně ze seznamu potenciálních kanálů odstraní ty kanály, které mají nadměrnou úroveň energie. [14]

Obrázek 4 ZigBee koordinátor [15]

6.2.2 Router

Router, taktéž nazývaný jako směrovač, hledá platnou ZigBee síť a po jejím nalezení se k ní musí připojit. Po připojení routeru k síti je umožněno dalším zařízením připojit se do ZigBee sítě. Router, stejně jako koordinátor, také může směrovat datové pakety a komunikovat s dalšími zařízeními v síti. [14]

Aby bylo možné zjistit dostupnost blízkých sítí ZigBee, router provede sken PAN. Během tohoto skenování router odešle požadavek synchronizačního rámce (beacon) přenosu na první kanál v seznamu skenovacích kanálů. Koordinátory a routery, které pracují na tomto prvním kanálu a jsou součástí sítě ZigBee, odpoví na požadavek synchronizačního rámce

odesláním rámce zpět do routeru. Pokud existuje platná ZigBee síť v dosahu, router se k ní obvykle připojí během několika sekund. [14]

Synchronizační rámec obsahuje informace o PAN, ve které je nebližší zapnuté zařízení, dále PAN identifikátor (PAN ID) i informaci o tom, zda je povoleno připojení. [14]

Router vyhodnotí každý synchronizační rámec přijatý na kanálu a rozhodne, zda našel platnou PAN. Síť je platná v případě, že je platná jedna z následujících možností:

- Má platné 64bitové ID PAN
- Má správný profil zásobníku
- Umožňuje připojení k síti [14]

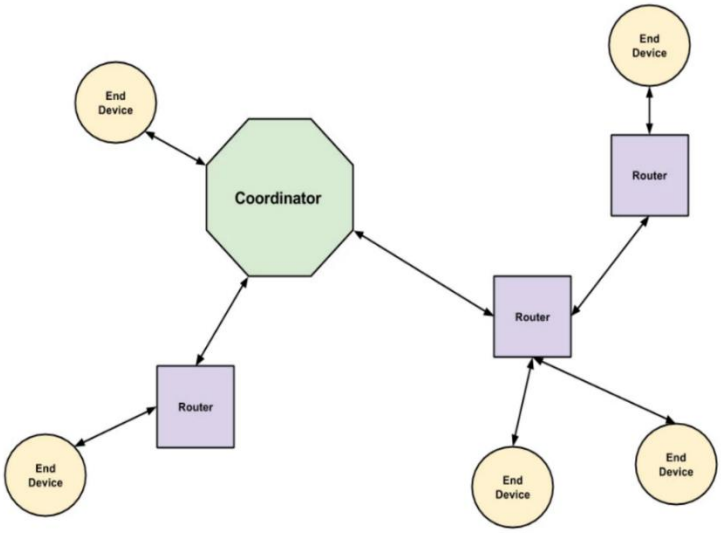
Pokud router nenajde platnou PAN, provede skenování na dalším kanálu v seznamu skenovacích kanálů. Ve skenování pokračuje, dokud nenajde platnou síť nebo dokud nejsou prohledány všechny kanály. Pokud router prohledá všechny kanály a nenajde platnou PAN, prohledá všechny kanály znovu. [14]

6.2.3 Koncové zařízení

Obdobně jako je tomu u směrovačů, koncová zařízení musí najít platnou ZigBee síť a připojit se k ní. Po připojení k síti je umožněna komunikace s ostatními zařízeními ve vytvořené síti ZigBee. Koncová zařízení jsou standardně napájená baterií. Kvůli úspoře energie jsou u koncových zařízení používány režimy s nízkou spotřebou. Tento typ zařízení v souvislosti s úsporou energie neumožňuje směrovat datové pakety a ani není možné k němu připojovat další zařízení. Z pohledu IEEE 802.15.4 se tedy jedná o zařízení s omezenou funkčností. [14]

Obrázek 5 Příklad koncového zařízení – vlhkostní a teplotní senzor ZigBee [16]

Varianty propojení jednotlivých zařízení jsou znázorněny na Obrázku 6.



Obrázek 6 Varianty propojení jednotlivých zařízení ZigBee [17]

6.2.4 Zabezpečení sítě

Komunikační technologie ZigBee podporuje dva bezpečnostní režimy:

- **Standardní režim** – je využíván na rezidenční použití. V tomto režimu zabezpečení Trust Center řídí zásady přístupu do sítě, udržuje seznam zařízení, hlavních klíčů, propojovacích klíčů, a síťových klíčů všech zařízení v síti. V tomto režimu musí mít každé zařízení, které žádá o přístup k síti, globální zabezpečovací klíč nebo jedinečný zabezpečovací klíč (v závislosti na konkrétním použití). Aby bylo zařízení zajištěno bezpečné připojení k síti, musí mít Trust Center dřívější záznam o hodnotě klíče a typu klíče. Výhoda globálního klíče spočívá v tom, že paměť využívaná Trust Center se nezvětšuje s rostoucím počtem zařízení v síti. Naopak jedinečný klíč má zase tu výhodu, že je jedinečný pro všechny zařízení připojené v síti a komunikace může být zabezpečena z jiných zařízení v síti. [18]
- **Režim vysokého zabezpečení** – je určený pro komerční aplikace s vysokým zabezpečením. V tomto režimu Trust Center udržuje seznam zařízení, hlavních klíčů, propojovacích klíčů a síťových klíčů. [18]

6.2.5 Trust center

ZigBee Trust Center je aplikace, která je spuštěna na důvěryhodném zařízení v síti ZigBee a je zodpovědná za autentizaci zařízení připojovaných k síti a za distribuci klíčů. Jako Trust Center může být nastaven například koordinátor. [18]

6.3 Zabezpečovací model

Zabezpečení se aplikuje na síťovou vrstvu a APS vrstvu. Pakety jsou šifrovány 128bitovým šifrováním AES. K šifrování dat je možné použít síťový klíč a volitelný propojovací klíč. V jedné síti spolu mohou komunikovat pouze ta zařízení, která mají stejné klíče. Směrovače a koncová zařízení, která budou komunikovat v zabezpečené síti, musí obdržet správné zabezpečovací klíče. [14]

Zabezpečení síťové vrstvy – Síťový klíč se používá k šifrování dat vrstvy APS a dat aplikací. Kromě šifrování aplikačních zpráv je zabezpečení sítě také aplikováno na směrovací zprávy a odpovědi, příkazy APS a příkazy ZDO. Síťový klíč se nepoužívá u přenosů na MAC úrovni, jako jsou přenosy synchronizačního rámce. [14]

- **Zabezpečení vrstvy APS** – Zabezpečení vrstvy APS lze použít k šifrování používaných dat pomocí klíče, který je sdílen mezi zdrojovým a cílovým zařízením. [14]

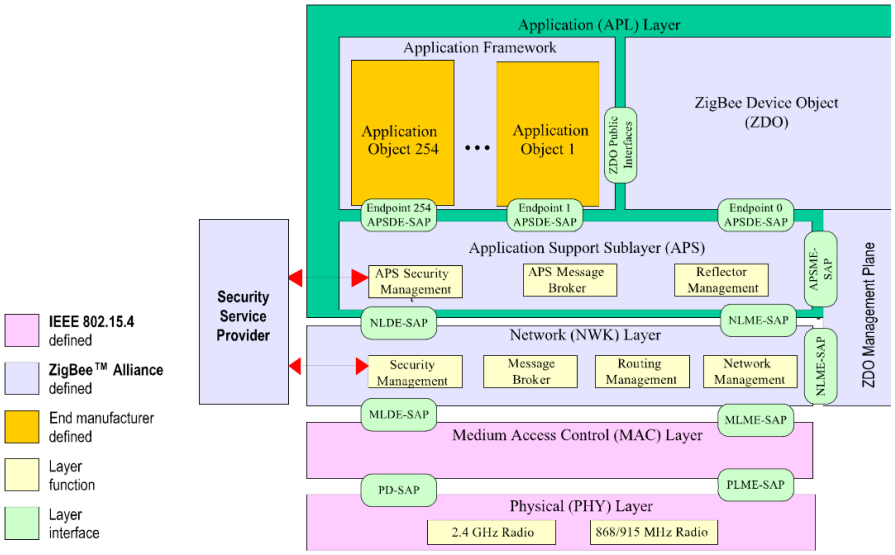
6.4 Vrstvy síťového modelu

Komunikace prostřednictvím bezdrátové komunikační technologie ZigBee se dá rozdělit do čtyř vrstev síťového modelu. [19]

Aplikační vrstva – Překládá pakety na data, se kterými je možné dále pracovat. Zprostředkovává tedy výměnu dat mezi uživatelem a síťovou vrstvou. Tato vrstva se celkově skládá ze dvou částí, které tvoří celek. Jedná se o podvrstvu podpory aplikace a podvrstvu, kterou definuje programátor vytvářející aplikaci využívající komunikační technologii ZigBee. [19]

- **Síťová vrstva**– Zprostředkovává směrování paketů na základě jejich cílové adresy. Zároveň má za úkol konfigurovat nové uzly a vytvářet kanál pro zabezpečené spojení. [19]

- **Linková vrstva –** Má za úkol zprostředkovávat přeposílání MAC rámců mezi dvěma bezprostředně propojenými uzly. Je založena na protokolu 802.15.4 MAC. [19]
- **Fyzická vrstva –** Tato vrstva využívá protokol IEEE 802.15.4 PHY, který je rozdílný pro pásma 868 MHz a 915 MHz či 2,4 GHz. Má za úkol zprostředkovávat výměnu dat mezi přenosovým médiem a linkovou vrstvou. Je zodpovědná za výběr kanálu a za ovládání rádiového vysílače a přijímače. [19]



Obrázek 7 Vrstvy síťové modelu ZigBee [20]

6.5 Směrování

Pro směrování se v této komunikační technologii využívá protokolu Ad hoc On-demand Distance Vector routing. Směrování se uskutečňuje na síťové vrstvě. Pokud se v dané síti použije hvězdicová topologie, o směrování se v každém případě postará koordinátor. Jestliže je použita stromová topologie nebo obecná síť, router i koordinátor musí pravidelně aktualizovat směrovací tabulky, které obsahují informace o cestě k danému uzlu, aby bylo možné reagovat na změny v dané síti. [19]

Další možností směrování je odeslání multicastové zprávy. Multicastová zpráva je zpráva, která se odešle všem uzlům, které patří do multicastové skupiny. [19]

7 Komunikační technologie Z-Wave

Protokol Z-Wave je interoperabilní bezdrátová komunikační technologie založena na RF komunikaci. Uplatňuje se především v řízení osvětlení, HVAC systémech, zabezpečovacích systémech, domácích kinech, automatickém ovládání oken a stínění a v neposlední řadě v přístupových systémech. Z-Wave je považován za lídra na světovém trhu v oblasti bezdrátové domácí automatizace. [21]

Obrázek 8 Logo Z-Wave [22]

7.1.1 Historie

Společnost Zen-Sys, založena v Dánsku na konci devadesátých let, byla první, která začala vyvíjet protokol Z-Wave. V roce 2003 uvedla jeho první generaci – kombinaci transceiveru se standardním mikrokontrolerem značky Atmel. Jelikož byla v USA automatizace již známá (díky protokolu ze 70. let 20. století X10), staly se Spojené státy prvními většími zákazníky společnosti. V Evropě se Z-Wave prvně uchytil u firmy Danfoss, která se specializuje na výrobu termostatů. Po dvou letech od uvedení Z-Wave na trh došlo k odkoupením Zen-Sys společností Sigma Designs (americká firma pro výrobu čipů) a následně i k masivnímu rozmachu jak na americkém, tak evropském i asijském trhu. Rok 2005 byl důležitý také pro to, že bylo založeno konsorcium Z-Wave Alliance, které zaštiťuje výrobu elektronických produktů s využitím protokolu Z-Wave. V Z-Wave Alliance je aktuálně členem více než 450 společností, kterým jsou zajišťována školení k rozšíření znalostí, certifikace jednotlivých zařízení i propagace jejich produktů. [19]

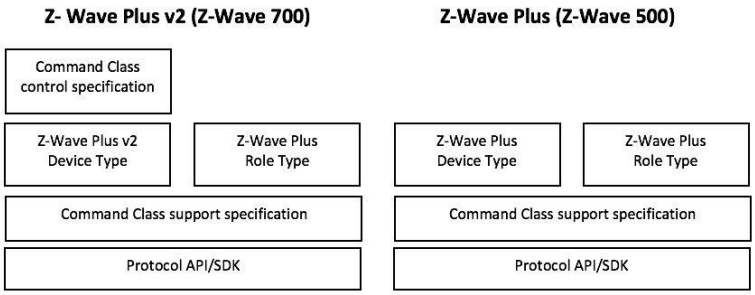
7.1.2 Z-Wave Alliance

Z-Wave Alliance byla založena počátkem roku 2005 předními výrobci regulačních komponentů pro domácnosti. Důvodem založení aliance byla jejich nespokojenost s tehdejším technologickým vývojem domácí automatizace a snaha o posunutí tohoto odvětví do každodenního života. [21]

Po několika letech snahy technologů o vytvoření standardu, na kterém by bylo možné stavět budoucí Z-Wave výrobky, se sešli zakládající členové firem Intermatic, Leviton, Wayne Dalton, Danfoss a Univesral Electronic s tvůrci společnosti Zensys, aby projednali možnosti související s dokončením standardu. Ihned po zahájení vývoje produktů s čipovou technologií Zensys si tito zakládající členové uvědomili, že konečně našli spolehlivý hardware s velkým tržním potenciálem. Výrobci komponentů domácího řízení se obrátili na společnost Zensys a společně se rozhodli vytvořit Alianci Z-Wave. [21]

7.2 Specifikace Z-Wave

Specifikace Z-Wave jsou aktualizovány čtyřikrát ročně. Každé vydání je označeno rokem a dopisem, jako: 2019A, 2019B, 2019C, 2019D. Aktuálně jsou na trhu k dispozici certifikace produktů řady 500 a 700. Výrobky řady 500 musí splňovat požadavky na certifikaci Z-Wave Plus, výrobky řady 700 požadavky na Z-Wave Plus v2. Hlavní rozdíl mezi řadami spočívá v tom, že řada 700 navíc obsahuje specifikaci pro řízení třídy příkazu (Command Class control specification, viz. Obrázek 9).Pro zajištění interoperability musí každý produkt projít certifikačním programem před uvedením na trh. [23]



Obrázek 9 Specifikace Z-Wave [24]

Před vydáním nové aktualizace je pro členy a partnery aliance po dobu 30 dní spuštěna otevřená recenze. Účelem je provedení kontroly aktualizace a poskytnutí zpětné vazby. V případě že se nenajdou žádné problémy, je toto období prodlouženo. [23]

7.3 Z-Wave síť

Každé zařízení v síti lze také nazvat uzlem. V jedné síti Z-Wave se může nacházet maximálně 232 uzlů. Pro použití více uzlů je potřeba připojit druhý kontrolér. Druhý kontrolér je ale nutné aplikačně propojit s prvním kontrolérem. [25]

Uzly dělíme na kontroléry a jim podřízené uzly. Kontroléry jsou obvykle v podobě ručních dálkových ovladačů nebo rozhraní v počítačích. Příklady podřízených uzlů jsou vypínače, stmívače, snímače pohybu atp. V síti uzlů si iniciátor (zdrojové zařízení, které chce vysílat) hledá vždy nejkratší možnou aktivní cestu, kde musí obcházet neaktivní překážky. Ta ve výsledku může být delší než přímá cesta iniciátor-příjemce. Zařízení v síti mohou být kdykoliv přidána či odebrána, což ze sítě činí dynamickou entitu. Po každé změně je využit systém zpětného upozornění, který všechna zařízení v síti o změně informuje. [25]

7.4 Identifikace uzlů

Zařízení Z-Wave jsou identifikována dvěma způsoby. První způsob je proveden pomocí 4bajtového home ID, které je přiřazováno kontrolérem zařízení během procesu párování. Všechny uzly spárované s daným kontrolérem sdílejí stejné home ID, které je kontroléru přiřazeno ve výrobě. [26]

Druhým způsobem identifikace je node ID. Node ID je hodnota bajtů přiřazená také kontrolérem zařízení během procesu párování. Uzel kontroléru má vždy hodnotu node ID jedna. První zařízení spárované s řadičem má node ID dva. Následné operace párování vždy zvyšují hodnotu node ID o jedna. [26]

7.5 Základní třídy zařízení

Všechna zařízení Z-Wave jsou vyčleněna prostřednictvím tříd zařízení. Funkce, které jsou v daném zařízení implementovány, závisí na třídách zařízení, do které je zařízení patří. [27] Jednotlivé kategorie tříd jsou popsány v následujících podkapitolách.

7.5.1 Basic Device Classes

Tato kategorie rozlišuje zařízení na:

- přenosný kontrolér
- statický kontrolér
- slave
- slave s možností směrování [28]

Přenosný kontrolér

Přenosný kontrolér je možno použít k ovládání jiných uzlů v síti Z-Wave. Pokud tento typ zařízení zůstane v přímém dosahu alespoň jednoho uzlu v síti, může být přesunut. Významnou vlastností tohoto zařízení je schopnost zahrnout ostatní zařízení do lokální sítě Z-Wave. Typické použití tohoto zařízení je například dálkové ovládání. Identifikátorem zařízení je BASIC_TYPE_CONTROLLER. Pro správnou funkčnost je nutné, aby aplikace na tomto zařízení podporovaly následující funkce:

- **Přiřazení adresy uzlu** – Přenosný kontrolér má možnost zařazovat nebo vyřazovat ostatní kontroléry a zařízení slave v rámci sítě Z-Wave. Tato schopnost vyžaduje, aby se jednalo o primární kontrolér. Nově zahrnuté řadiče v síti se nazývají sekundární řadiče. [28]
- **Plné směrování** – Toto zařízení musí podporovat úplnou směrovací část protokolu Z-Wave. To zahrnuje shromažďování informací o uzlu, udržování směrovací tabulky, vytváření směrovacích seznamů a používání směrovacích seznamů pro přenos dat. Kontrolér nepřebírá určitou pozici v síti, ale pokouší se zjistit, které uzly jsou přímo v dosahu a je možné je použít pro směrování dále do sítě. [28]
- **Replikování řadičů dat souvisejících s protokolem** – Přenosný řadič musí být schopen kopírovat informace o uzlu, informace o směrování a další data související s protokolem jiného řadiče v síti Z-Wave [28]

Statický kontrolér

Statický kontrolér je přizpůsoben zařízením, která jsou síti Z-Wave pevně umístěna. Zařízení může sloužit jako přijímač například pro senzory nebo jiná zařízení napájená baterií, která musí odesílat zprávy do kontroléru. Může být také použit v systému, kde kontrolér potřebuje

znát stav každého řízeného zařízení v síti. Vzhledem k tomu, že tento typ kontroléru je schopný se naučit a uložit nejlepší trasu do všech uzlů v systému, výrazně snižuje latenci ve větších systémech. Identifikátorem tohoto zařízení je BASIC_TYPE_STATIC_CONTROLLER. Pro správnou funkčnost je nutné, aby aplikace na tomto zařízení podporovaly následující funkce:

- Přiřazení adresy uzlu
- Plné směrování
- **Podpora směrovače** – Statický kontrolér má schopnost fungovat jako směrovač, v případě pokusu zdrojového uzlu o dosažení cílového uzlu mimo přímý rozsah
- Replikování řadičů dat souvisejících s protokolem [28]

Slave

Slave je nejjednodušším uzlem v síti Z-Wave. Tento uzel není schopen za normálních okolností zahájit přenos dat do jiných uzlů v síti Z-Wave. K přenosu může dojít pouze v případě, pokud se jedná o odpověď na požadavek. Typickou realizací slave může být světelný stmívač nebo router. Identifikátorem tohoto zařízení je BASIC_TYPE_SLAVE. Pro správnou funkčnost je nutné, aby aplikace na tomto zařízení podporovaly následující funkce:

- **Přidání nebo odebrání uzlu –** Slave musí mít schopnost být přidán (případně být odstraněn) v síti Z-Wave primárním nebo sekundární kontrolérem
- Podpora směrovače [28]

Slave s možností směrování

Slave s možností směrování má v podstatě stejnou funkci jako slave, ale uzel má navíc možnost zahájit přenos dat do omezeného počtu dalších uzlů v síti Z-Wave. Toto zařízení může být napájeno ze sítě i z baterie. Typickou aplikací může být pohybový detektor. Slave s možností směrování je možno dále upravit s využitím externího EEPROM pro ukládání dat aplikací. Zařízení je pak možno použít jako tlačítko, detektor pohybu nebo teplotní senzor. Identifikátorem tohoto zařízení je BASIC_TYPE_ROUTING_SLAVE. Pro správnou funkčnost je nutné, aby aplikace na tomto zařízení podporovaly následující funkce:

- Přidání nebo odebrání uzlu
- Podpora směrovače [28]

7.5.2 Generic Device Classes

Hlavní funkcionalitu daných zařízení určuje Generic Device Class. Konkrétně tedy určí, o jaký druh zařízení se jedná. Tuto třídu doplňuje Specific Device Class, která ještě přesněji druh zařízení specifikuje. [27] Druhem generického zařízení může být například:

- Binární senzor (identifikátorem je GENERIC_TYPE_SENSOR_BINARY)
- Termostat (identifikátorem je GENERIC_TYPE_THERMOSTAT)
- Ventilace (identifikátorem GENERIC_TYPE_VENTILATION) [29]

7.6 FLiRS

Mnoho typů snímačů zabezpečení napájených baterií (senzory dveří, oken a pohybu) dosahují dlouhé životnosti baterie, protože jsou většinu času v úsporném režimu. Probuzeny jsou až ve chvíli, kdy je provedena nějaká akce (například rozpojení kontaktů). Existují však typy zařízení, která nemohou zůstat dlouhou dobu v režimu spánku – musí stále přijímat signály. Z tohoto důvodu byl vyvinut FLiRS. Zařízení s touto implementací jsou schopna omezit spotřebu energie na 50μA/hod a méně. [30]

Pokud kontrolér Z-Wave nebo jiný uzel v síti potřebuje komunikovat se zařízením napájeným z baterie (jako je například zámek dveří) odešle kontrolér speciální signál (beam signal) do požadovaného uzlu. Tento signál má za úkol probudit konkrétní zařízení. Zařízení, ve kterém je implementován FLiRS cyklicky střídá režim spánku a režim částečného probuzení. V režimu částečného probuzení naslouchá signálu pro probuzení. V případě obdržení tohoto signálu se zařízení okamžitě zcela probudí a může tak komunikovat s kontrolérem nebo jiným zařízením Z-Wave s využitím standardních příkazů protokolu. Pokud zařízení signál nepřijme, vrátí se do plného režimu spánku, dokud se znovu částečně neprobudí a nenaslouchá. FLiRS tímto vytváří režim, který zajišťuje životnost baterie na stejné úrovni jako je plně spící zařízení a zároveň poskytuje komunikační latenci přibližně jednu sekundu. [30]

7.7 Třídy příkazů

Třídy příkazů představují funkce určitého zařízení Z-Wave. Každý typ zařízení (přepínače, stmívače, termostaty) podporuje různé třídy příkazů. Aby bylo zajištěno, že zařízení Z-Wave mohou vzájemně komunikovat, i když neznají konkrétní funkci druhého zařízení, existuje speciální třída příkazů s názvem Basic. Třída příkazů Basic se skládá ze dvou příkazů a jedné odpovědi:

- SET – nastaví hodnotu mezi 0 a 255
- GET – požádá zařízení, aby nahlásilo hodnotu
- REPORT – odpověď na příkaz GET, hlášení hodnoty mezi 0 a 255 [29]

Jedinečnou vlastností třídy příkazů Basic je, že každé zařízení interpretuje příkazy Basic v závislosti na konkrétních funkcích tohoto zařízení. Například binární přepínač se zapne po přijetí hodnoty 255 a vypne při hodně 0, termostat přejde například do režimu pohodlí, když přijme hodnotu 0 a do režimu úspory energie přejde při přijetí jakékoliv jiné hodnoty. [29]

Obrázek 10 Třída příkazů Basic [31]

Každý příkaz lze zařadit do tzv. command class (třídy příkazů), do které patří právě takové příkazy, které jsou spojené s funkcionalitou, kterou reprezentuje. Každé zařízení poskytuje seznam podporovaných command classes pomocí NIF. [27] [29]

7.8 Zabezpečení

Využití zabezpečovací vrstvy bylo v minulosti volitelné a úměrné účelu konkrétního zařízení. Po zabezpečovacích problémech Z-Wave však zavedlo certifikaci Security 2 pro všechny produkty. To znamená, že S2 zabezpečuje komunikaci jak lokálně pro domácí nebo obchodní zařízení, tak v rozbočovači nebo bráně pro cloudové funkce. Toto zabezpečení komunikace prakticky odstraňuje riziko napadení zařízení v době, kdy jsou připojena k síti.

S2 totiž implementuje zabezpečenou výměnu klíčů v celém odvětví pomocí ECDH, což prakticky znemožňuje rozluštění síťového klíče. [32]

Zařízení jsou rozdělena do dvou tříd. Zařízení pro řízení přístupu, jako jsou dveřní zámky, musí být během zařazení do sítě ověřena. Zařízení z druhé třídy si mohou vybrat mezi tím, zda budou během přidávání do sítě ověřena či nikoliv. S2 umožňuje tunelování všech přenosů Z-Wave přes IP přes zabezpečené tunely TLS 1.1, což eliminuje také zranitelnost cloudových přenosů. [32]

8 Porovnání bezdrátových komunikačních technologií ZigBee a Z-Wave

Technologie ZigBee a Z-Wave jsou dva z nejvýznamnějších bezdrátových protokolů používaných v produktech chytré domácnosti. Nejde je však spojit dohromady a přes všechny své podobné vlastnosti mají klíčové rozdíly. A právě těmito rozdíly se zabývá tato kapitola.

8.1 Fyzikální rozdíly

8.1.1 Topologie

Z hlediska topologie nejsou v jednotlivých technologiích příliš velké rozdíly, jelikož obě spadají do standardu IEEE 802.15.4. Oba standardy využívají pro komunikaci smíšenou topologii (mesh).

Přes to, že ZigBee i Z-Wave fungují na stejném standardu, nelze jednotlivá zařízení daných technologií mezi sebou vzájemně propojovat. To znamená že Z-Wave síť je možné složit ze zařízení Z-Wave a ZigBee síť pouze ze zařízení ZigBee. Výrazný rozdíl, který lze zahrnout do topologie je dosah. Z-Wave může připojit zařízení do vzdálenosti až 30 metrů, zatímco ZigBee maximálně 10 metrů. Tento parametr technologii ZigBee oproti Z-Wave poněkud znevýhodňuje. Pro stabilní připojení je totiž nutné tuto vzdálenost dodržet. Z toho vyplývá požadavek na rozmístění zařízení ZigBee v každé místnosti domácnosti, což by v případě většího objektu mělo negativní vliv na finance spotřebitele. [33]

Vzhledem k obecné topologii, není nutné připojovat jednotlivá zařízení přímo k rozbočovači. Namísto toho stačí každé zařízení připojit k nejbližšímu zařízení ve svém dosahu. Signál pak přejde z jednoho zařízení na druhé a je tak tvořena cesta až k rozbočovači. U technologie Z - Wave je zde však omezení v počtu skoků mezi jednotlivými uzly. Z-Wave zařízení dokáže provést maximálně čtyři skoky. To znamená, že pokud jsou nejbližší tři zařízení příliš daleko od sebe, je cesta přerušena a spojení je ztraceno. ZigBee však může procházet tolik zařízení, kolik je zrovna potřeba k dosažení rozbočovače. Což určitým způsobem řeší problém s jejím krátkým dosahem. V případě že by spotřebitel plánoval instalovat do objektu řadu chytrých senzorů, žárovek, zámků apod., ZigBee představuje snadnější zajištění stability sítě. [33] [34]

8.1.2 Frekvence

Zařízení ZigBee pracují v nelicencovaných pásmech ISM. Nejpoužívanější konfigurací je frekvence na 2,4 GHz, kde standard definuje šestnáct 5MHz kanálů pro provoz. Maximální přenosová rychlost je 250kbit/s s využitím OQPSK. Další specifikace umožnují provoz na 915 MHz (v USA) s přenosovou rychlostí 40 kbit/s s využitím BPSK. Evropská verze pak používá frekvenci 868 MHz s přenosovou rychlostí 20 kbit/s. [33]

Technologie Z-Wave taktéž využívá nelicencované pásmo ISM. V Evropě pracuje na frekvenci 868,42 MHz. V USA a Kanadě pracuje primárně na frekvenci 908,42 MHz. V jednotlivých státech se může na základě předpisů frekvence lišit. Modulace funguje na principu klíčování frekvenčním posunem (FSK). Přenosová rychlost na těchto frekvencích dosahuje přibližně 40kbit/s. [33]

Obě technologie tedy využívají nelicencovaná pásma ISM. Rozdíl je však v přenosové rychlosti evropských verzí ZigBee a Z-Wave a ve způsobu modulace. Zatímco Z-Wave dosahuje rychlosti 40kbit/s s modulací FSK, ZigBee pouze 20 kbit/s, tedy poloviční přenosové rychlosti oproti Z-Wave (frekvence evropských zařízení obou technologií je znázorněna na Obrázku 1). [33]

8.1.3 Spotřeba

U koncových zařízení obou technologií je pro provoz jedním z klíčových parametrů spotřeba, jelikož jsou napájena pomocí baterie. Obě technologie se tak řadí mezi nízkoenergetické. V minulosti byla spotřeba u ZigBee menší, ale s vývojem obou zařízení se spotřeba velmi snížila a dosahuje řádově desítek μA/hod. Tento parametr není tedy při výběru technologie relevantní.

Obě technologie využívají různé režimy pro úsporu energie. Z-Wave pro tyto účely vyvinulo zařízení FLiRS, které cyklicky střídá režim spánku a režim částečného probuzení, čímž je docíleno výrazné úspory energie. Koncová zařízení ZigBee fungují obdobně. Využívají buď krátké spánkové periody nebo dlouhé spánkové periody. Při krátké spánkové periodě jsou koncová zařízení schopna zpětně reagovat na dotaz (díky ukládání dotazů do vyrovnávací paměti nadřazeného zařízení). U dlouhé spánkové periody je reagování na dotaz složitější. [14]

8.1.4 Shrnutí fyzikálních rozdílů

Následující tabulka shrnuje a hodnotí výše uváděné parametry.

Parametr	ZigBee	Z-Wave
Topologie	Smíšená	Smíšená
Dosah	max 10 m	až 30 m
Maximální počet skoků mezi uzly	neomezeně	4
Frekvence	868 MHz	868,42 MHz
Pásmo	bezlicenční ISM	bezlicenční ISM
Přenosová rychlost	20 kbit/s	40 kbit/s
Spotřeba	řádově desítky µA/hod	řádově desítky µA/hod
Modulace	OQPSK/BPSK	FSK

Tabulka 2 Shrnutí fyzikálních rozdílů [vlastní]

Z tabulky lze vyčíst, že z hlediska fyzikálních rozdílů se komunikační technologie ZigBee a Z-Wave příliš neliší, avšak jsou zde podstatné rozdíly. Dosah ZigBee je sice výrazně menší než u Z-Wave ale tento parametr není při výběru technologie klíčový. Záleží na typu konkrétní instalace. Problém by mohl nastat pouze v případě, pokud by technologie byla instalována do většího objektu, kde by vzdálenost mezi jednotlivými zařízeními přesáhla vzdálenost 10 metrů a uživatel nechtěl mít zařízení ZigBee v každé místnosti. Dosah by v tomto případě zcela jistě nestačil.

Určitou výhodou ZigBee je maximální počet skoků mezi jednotlivými uzly v síti. To znamená, že pokud jsou 3 nejbližší zařízení příliš daleko od sebe, ZigBee je schopno najít cestu k rozbočovači přes jiné uzly. V případě Z-Wave by bylo spojení ztraceno.

Přenosová rychlost na evropské frekvenci je u Z-Wave jednoznačně vyšší než u ZigBee, ale vzhledem k oblasti využití obou technologií není tento parametr příliš významný.

8.2 Aplikační rozdíly

8.2.1 Standard

ZigBee i Z-Wave jsou založeny na standardu 802.15.4. přičemž tento standard definuje u komunikační technologie ZigBee fyzickou a MAC vrstvu. ZigBee je otevřený standard vyvinutý ZigBee Aliancí. Oproti tomu Z-Wave je vyvinut společností Zensys jako proprietární, bezdrátový a uzavřený standard. Mezinárodní telekomunikační unie (ITU)

přidává fyzickou a MAC vrstvu ve standardu G.9959. V roce 2020 by však mělo dojít ke změně a ze Z-Wave by se měl stát také otevřený standard. [35] [36]

8.2.2 Aliance

Komunikační technologie ZigBee je udržována ZigBee Aliancí. Jedná se o konsorcium společností a dalších organizací, které podporují vývoj standardu a podporují jeho používání. Aliance provádí řadu testování, aby potvrdila, že všechny produkty splňují normu. Díky tomu, že je ZigBee otevřený standard, je jednou z jeho výhod velká flexibilita. Existuje tedy mnoho výrobců zařízení – Ember, Microchip, Atmel, Digi a další. Pro ZigBee byl navržen specifický aplikační software známý jako „profily“. Profily se připojují k zásobníku ZigBee a usnadňují výrobcům vytváření bezdrátových produktů pro velmi specifické aplikace. [33]

Oproti tomu, Z-Wave, je udržována Z-Wave Aliancí. Jedná se o konsorcium zahrnující více než 700 společností, které navrhují a prodávají bezdrátové produkty pro domácí automatizaci založené na technologii Z-Wave a důkladně prověřuje jejich kvalitu. [33]

8.2.3 Integrovatelnost

ZigBee

Firmy Ember a iControl se spojily za účelem pomoci poskytovatelům širokopásmových služeb a domácím zabezpečovacím společnostem pokračovat v trendu interaktivních služeb zabezpečení, monitorování a domácí správy. Společně vyvinuli softwarovou platformu iControl OpenHome, která je schopna spárovat svou otevřenou softwarovou infrastrukturu s dotykovou obrazovkou all-in-one. Kombinuje zabezpečovací systém, komunikační bránu a platformu domácí automatizace ZigBee do jednoho zařízení. Tím byla vytvořena platforma, která poskytuje obousměrnou bezdrátovou infrastrukturu pro celou síť ZigBee. V současné době však existují i další zařízení, která kombinují veškerá zařízení ZigBee do jednoho. [33]

Z-Wave

U technologie Z-Wave taktéž existují možnosti, jak spojit veškerá zařízení v síti do jednoho virtuálního a ovládat jím celý objekt. Ve většině případů je k tomuto účelu zapotřebí centrální jednotka, ke které se následně připojují ostatní periferie – například Fibaro Home Center 2. [37]

8.2.4 Oblasti využití

ZigBee

Dostupné profily zahrnují domácí automatizaci, inteligentní energii, telekomunikaci, zdravotní péči, dálkové ovládání (RF4CE nebo rádiovou frekvenci pro spotřební elektroniku), automatizaci budov a maloobchodní služby. Oblast použití ZigBee je tedy velice široká. [36]

Z-Wave

Aliance nabízí více než 3000 produktů, které jsou primárně zaměřeny na zabezpečení a ovládání domácností a malých komerčních zařízení (to zahrnuje řízení osvětlení, ovládání zabezpečovacích zařízení a řízení vzduchotechniky). V porovnání se ZigBee má Z-Wave oblast použití menší. [36]

8.2.5 Bezpečnost

Jak Zigbee, tak Z-Wave donedávna používali standard šifrování AES 128, což je standardizovaný algoritmus používaný k šifrování dat v informatice. Je to stejný algoritmus, který využívají například bezdrátové sítě Wi-Fi v rámci zabezpečení WPA2. [38]

Z-Wave Aliance však v minulosti čelila obvinění z bezpečnostních výpadků, které byly způsobeny chybou některé z firem vydávající zařízení Z-Wave. Firma totiž nevyužila vysokou úroveň šifrování. Po tomto obvinění Z-Wave Aliance vydala požadavek na certifikaci S2. To znamená, že je pro všechny výrobce Z-Wave zařízení je nyní povinné do zařízení implementovat nejnovější Security 2 rámec. [32]

S2 používá strukturu jednoho příkazu, který nahrazuje předchozí čtyřstupňový proces u AES 128, který snižuje latenci a zlepšuje životnost baterie pro zařízení používající novou architekturu zabezpečení. Již dříve měly sítě Z-Wave pro každou síť jedinečné bezpečnostní klíče. S2 toto opatření vylepšuje tím, že má také jedinečné klíče, ale pro každou skupinu zařízení. Jedinečné síťové klíče zajišťují, že informace z jedné sítě nelze použít k dešifrování jiné sítě. [32]

ZigBee však stále používá standard šifrování AES 128, jehož algoritmus zahrnuje 4 fáze. To určitým způsobem snižuje latenci a zvyšuje nároky na energii. Tento standard zabezpečení

se dá považovat za relativně bezpečný, ale ve srovnání se současným šifrováním Z-Wave je ZigBee pozadu. [32]

8.3 Shrnutí aplikačních rozdílů

ZigBee a Z-Wave se zaměřují na velmi podobné obecné aplikace. ZigBee je však zdaleka více univerzální, protože může být nakonfigurováno pro prakticky jakýkoliv dotaz bezdrátové úlohy. Profily ZigBee jsou snadno dostupné a tím je minimalizována doba vývoje běžných aplikací. Na druhou stranu je tento protokol je mnohem složitější.

Určitou nevýhodou Z-Wave oproti ZigBee je druh standardu. Nejedná se totiž zatím o otevřený standard. U ZigBee i Z-Wave je možnost propojení veškerých zařízení v objektu se stejnou technologií do jednoho zařízení a ovládat tak domácnost například pomocí tabletu.

Oblasti použití jednotlivých zařízení se nepatrně liší. Díky ZigBee profilům, které zahrnují domácí automatizaci, řízení spotřeby energie, telekomunikaci, zdravotní péči a dálkové ovládání, je oblast použití poměrně široká. Na druhou stranu, ZigBee, se primárně využívá pro zabezpečení a ovládání domácností či malých komerčních zařízení, což zahrnuje řízení osvětlení, ovládání zabezpečovacích zařízení a řízení vzduchotechniky. ZigBee je tedy z hlediska oblasti použití více univerzální

Zabezpečení technologií je jednoznačně kvalitnější u Z-Wave díky využití vrstvy S2. Z - Wave tak využívá jedinečné klíče pro každou skupinu zařízení, což zajišťuje, že informace z jedné sítě nelze použít k dešifrování jiné sítě. Z-Wave Aliance navíc zavedla certifikaci S2 na všechna zařízení využívající tuto technologii, což ji oproti ZigBee upřednostňuje.

8.4 Perspektiva vývoje technologií ZigBee a Z-Wave

Do budoucna se dá očekávat, že se obě tyto technologie budou neustále vyvíjet. Je to dáno především současným trendem automatizace, který se v dnešní době implementuje do velkého množství odvětví, přičemž domácnosti nejsou výjimkou. Dalším důvodem vývoje jsou rozrůstající se Aliance obou technologií. Dá se předpokládat, že noví členové Aliancí budou přinášet iniciativu k rychlé evoluci a inovacím těchto technologií.

Možnou inovací bezdrátové technologie ZigBee je zcela určitě zabezpečení. To je vzhledem k absenci vrstvy S2 ve srovnání se zabezpečením Z-Wave horší. Pro cílového zákazníka je

bezpečnost klíčová a vývojáři zařízení (nejen) pro chytré domácnosti si ve většině případů kladou velice vysoké nároky na zabezpečení. Vzhledem k tomu, že technologie ZigBee a Z - Wave si konkurují se tedy dá očekávat, že ZigBee nebude chtít být v ohledu bezpečnosti pozadu.

Dá se předpokládat, že určitým přínosem pro Z-Wave bude přechod z uzavřeného na otevřený standard. Proprietární povaha standardu a single-party výrobní strategie byla dlouhou dobu důvodem k mnoha diskusím. Integrace je často nákladnější než u konkurence. Podle dostupných zdrojů se v druhé polovině roku 2020 stanou dvě zásadní změny. Společnost Silicon Labs se odpojí od Z-Wave Aliance a stane se z ní samostatná organizace, která se bude chovat spíše jako normalizační orgán a bude pokračovat v produktové certifikaci. Další změnou je to, že Z-Wave bude otevřená tomu, aby konkurenti vyvíjeli a vyráběli svá vlastní zařízení. V případě, že se ze Z-Wave stane otevřený standard, bude zahrnovat rádiovou specifikaci, aplikační vrstvu, síťovou vrstvu a komunikační protokol hostitelského zařízení. [35]

9 Závěr

Cílem této práce bylo stručně a přehledně popsat bezdrátové komunikační technologie ZigBee a Z-Wave a poté provést jejich vzájemné porovnání. Nejprve je tedy v práci stručně popsána problematika bezdrátového přenosu dat a standardu IEEE 802.15.4, která s těmito technologiemi bezprostředně souvisí.

Při porovnávání technologií na základě fyzikálních, aplikačních a bezpečnostních rozdílů bylo zjištěno, že se příliš neliší. Avšak určité rozdíly zde pochopitelně existují. Z fyzikálního hlediska byl rozdíl zjištěn především ve frekvenci, dosahu, přenosové rychlosti a modulaci, přičemž nejpodstatnějším parametrem je dosah, který je u Z-Wave výrazně vyšší. Tuto technologii je tedy vhodné instalovat do objektů, které jsou větších rozměrů a nepředpokládá se, že bude mezi jednotlivými uzly sítě vzdálenost menší než 10 metrů.

Porovnávání technologií na základě aplikačních rozdílů bylo provedeno podle standardu, Aliance, oblasti použití, integrovatelnosti a bezpečnosti. Bylo zjištěno, že u technologie ZigBee je z aplikačního hlediska bezpochyby výhodou velké množství dostupných profilů, které výrobcům značně usnadňují vytváření bezdrátových produktů pro velmi specifické aplikace. Díky tomu je ZigBee velice univerzální protokol a je možné ho využít ve zdravotnictví, v chytrých domácnostech nebo pro telekomunikační služby. Z-Wave je v tomto ohledu omezen pouze na chytré domácnosti.

Z hlediska bezpečnosti je Z-Wave napřed díky povinnému používání zabezpečovací vrstvy S2, což z ní dělá velmi obtížně napadnutelnou komunikační technologii pro domácí automatizaci. Vzhledem k tomu, že si ZigBee a Z-Wave konkurují, lze do budoucna předpokládat inovaci ZigBee v podobě povinné implementace zabezpečovací vrstvy S2.

Na základě provedené analýzy informací a následného porovnání technologií nelze v současné době jednoznačně určit, která z technologií je lepší. Vždy bude záviset na konkrétní aplikaci technologie a bude potřeba zvážit řadu okolností (rozměry objektu, účel použití, množství uzlů v síti atp.), podle kterých bude vybrána technologie vyhovující požadavkům uživatele.

10 Seznam literatury

[1] SAJVERA, Miroslav. *Bezdrátové sítě a jejich zabezpečení* [online]. Hradec Králové, 2015 [cit. 2020-04-03]. Dostupné z: https://theses.cz/id/322io7/. Bakalářská práce. Fakulta informatiky a managementu, Katedra informačních technologií.

[2] PETERKA, Jiří. Bezdrátové přenosy. *CHIPweek* [online]. b.r., **96**(47) [cit. 2020-04-03]. Dostupné z: http://www.earchiv.cz/a96/a647k150.php3

[3] Elektromagnetické spektrum. In: *Archiv článků a přednášek Jiřího Peterky* [online]. 1996 [cit. 2020-04-04]. Dostupné z: http://www.earchiv.cz/a96/gifs/p647k151.gif

[4] *Sbírka zákonů Česká republika*. In: . Břeclav: Moraviapress, 2017, ročník 2017, částka 150, číslo 423.

[5] *Teorie datového IR přenosu* [online]. b.r. [cit. 2020-04-03]. Dostupné z: https://vyvoj.hw.cz/teorie-a-praxe/dokumentace/teorie-datoveho-ir-prenosu.html

[6] HYNČICA, Ondřej a Karel PAVLATA. Bezdrátové komunikační systémy založené na IEEE 802.15.4 v procesní automatizaci (1. část). *Automa* [online]. b.r. [cit. 2020-04-03]. Dostupné z: https://automa.cz/cz/casopis-clanky/bezdratove-komunikacni-systemy-zalozene-na-ieee-802-15-4-v-procesni-automatizaci-1-cast-2011_04_43411_5186/

[7] ZACHR, Václav. *Vrstva řízení přístupu k médiu standardu IEEE 802.15.4 ve vývojovém prostředí vestavných systémů* [online]. Brno, 2008 [cit. 2020-04-03]. Dostupné z: https://is.muni.cz/th/v9b0t/thesis.pdf. Diplomová práce. Masarykova univerzita, Fakulta informatiky.

[8] The ZigBee Home Automation Protocol - Specs and Benefits. *BuildYourSmarthome.co* [online]. 2018, (1) [cit. 2020-02-19]. Dostupné z: https://buildyoursmarthome.co/home-automation/protocols/zigbee/

[9] Průmyslové bezdrátové sítě ZigBee. *Automa*. 2009, **2009**(8-9), 73.

[10] Cesta k bezdrátové komunikaci – které standardy jsou nejlepší?. *Automa* [online]. 2018, **2018**(5), 46-47 [cit. 2020-02-19]. Dostupné z: https://automa.cz/Aton/FileRepository/pdf_articles/11502.pdf

[11] JUDGE, Peter. ZigBee logo. In: *Silicon.co.uk* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.silicon.co.uk/wp-content/uploads/2012/12/Zigbee-logo.jpg

[12] ZigBee Alliance. *IoT ONE* [online]. b.r. [cit. 2020-02-19]. Dostupné z: https://www.iotone.com/organization/zigbee-alliance/o206

[13] *ZigBee Alliance* [online]. b.r. [cit. 2020-02-19]. Dostupné z: www.zigbeealliance.org/

[14] *XBee®/XBee-PRO S2C Zigbee®: RF Module*. 2020.

[15] ZigBee koodinátor. In: *MATRIX* [online]. b.r. [cit. 2020-02-20]. Dostupné z: https://www.matrixtsl.com/webshop/e-blocks-zigbee-coordinator-board.html

[16] Multi-channel ZigBee Sensor with Battery Power Supply. In: *A2s.pl: AUTOMATION 2 SOLUTION* [online]. b.r. [cit. 2020-04-04]. Dostupné z: http://www.a2s.pl/products/zigbee/zs10/zs-10_small.jpg

[17] ZigBee Functional Descriptors. In: *KUDELSKI SECURITY.com: Research* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://cybermashup.files.wordpress.com/2017/11/zigbee-2.png

[18] *ZIGBEE SECURITY: BASICS: PART 1* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://research.kudelskisecurity.com/2017/11/01/zigbee-security-basics-part-1/

[19] FABIAN, Milan. *Bezdrátová síť ZigBEE pro sběr fyzikálních dat* [online]. Brno, 2013 [cit. 2020-04-03]. Dostupné z: https://is.muni.cz/th/olgli/text_prace.pdf. Bakalářská práce. Masarykova univerzita, Fakulta informatiky.

[20] Outline of the ZigBee Stack Architecture. In: *KUDELSKI SECURITY.com: Research* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://cybermashup.files.wordpress.com/2017/11/zigbee-1.png

[21] *About Z-Wave Technology* [online]. b.r. [cit. 2020-04-03]. Dostupné z: https://z-wavealliance.org/about_z-wave_technology/

[22] Z-Wave logo. In: *Z-Wave: Safer. Smarter.* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.z-wave.com/assets/logo-header.svg

[23] *Z-Wave Specification* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.silabs.com/products/wireless/mesh-networking/z-wave/specification

[24] Z-Wave Specification: Graphic. In: *SILICON LABS: Z-Wave Specification* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://siliconlabs-h.assetsadobe.com/is/image//content/dam/siliconlabs/images/products/Bluetooth/z-wave/z-wave-specification-graphic.png?$LargeFullContentWidth$

[25] *Introduction to OpenZWave* [online]. In: . b.r. [cit. 2020-04-04]. Dostupné z: http://www.openzwave.com/dev/

[26] BADENHOP, Christopher, Scott GRAHAM, Benjamin RAMSEY, Barry MULLINS a Logan MAILLOUX. *The Z-Wave routing protocol and its security implications. Computers & Security* [online]. b.r., **68** [cit. 2020-04-04]. DOI: 10.1016/j.cose.2017.04.004. ISSN 01674048. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0167404817300792

[27] LAUTERBACH, Michal. *Software pro měření elektromagnetické kompatibility* [online]. Pardubice, 2014 [cit. 2020-04-04]. Dostupné z: https://theses.cz/id/34wbpb/. Bakalářská práce. Univerzita Pardubice, Fakulta elektrotechniky a informatiky.

[28] *Software Design Specification: Z-Wave Device Class Specification* [online]. In: . b.r. [cit. 2020-04-04]. Dostupné z: https://www.silabs.com/documents/login/miscellaneous/SDS10242-Z-Wave-Device-Class-Specification.pdf

[29] *How Z-Wave Controllers & Devices Work* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.vesternet.com/pages/how-z-wave-controllers-devices-work

[30] *Z-Wave FLiRS: Enabling Wireless Smart Door Locks and Thermostat* [online]. In: . b.r. [cit. 2020-04-04]. Dostupné z: https://www.silabs.com/documents/login/white-papers/Z-Wave-FLiRS.pdf

[31] How Z-Wave Controllers & Devices Work: Basic Command Class. In: *Vesternet* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://cdn.shopify.com/s/files/1/0066/8149/3559/files/Z-Wave_Basic_Class.png

[32] WONG, William G. *Q&A: The Lowdown on Z-Wave's S2 Security Support* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.electronicdesign.com/technologies/embedded-revolution/article/21805285/qa-the-lowdown-on-zwaves-s2-security-support

[33] FRENZEL, Lou. *What's The Difference Between ZigBee And Z-Wave?* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.electronicdesign.com/technologies/communications/article/21796052/whats-the-difference-between-zigbee-and-zwave

[34] HENDRICKSON, Josh. *ZigBee vs. Z-Wave: Choosing Between Two Big Smarthome Standards* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.howtogeek.com/394567/zigbee-vs.-z-wave-choosing-between-two-big-smarthome-standards/

[35] TOOMBS, Cody. *Z-Wave spec will become open standard in 2020, allows companies to make Z-Wave chips* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.androidpolice.com/2019/12/19/z-wave-spec-become-open-standard/?fbclid=IwAR3SejgMi-kae0B6nWCVC5a09xr2DfuS7wxBwKqynTqpWuf3XJBj_YuIgE8

[36] *Home of RF and Wireless Vendors and Resources* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.rfwireless-world.com/Terminology/zigbee-vs-Z-wave.html?fbclid=IwAR2AxB_MX84WJN43ubSxX86r-OTfEFfOne6wIFBYkQ7Sl8nPVC2beaaP0uY

[37] *FIBARO Home Center 2: Black* [online]. b.r. [cit. 2020-04-04]. Dostupné z: https://www.alza.cz/fibaro-home-center-2-black-d5314564.htm

[38] Advanced Encryption Standard. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2020-04-04]. Dostupné z: https://cs.wikipedia.org/wiki/Advanced_Encryption_Standard?fbclid=IwAR3SejgMikae0B6nWCVC5a09xr2DfuS7wxBwKqynTqpWuf3XJBj_YuIgE8

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AES	Advanced Encryption Standard
APS	Application support sublayer
BPSK	Binary-Phase Shift Keying
ČTU	Český telekomunikační úřad
D2D	Device-to-Device
ECDH	Elliptic-curve Diffie–Hellman
EEPROM	Electrically Erasable Programmable Read-Only Memory
FFD	Full-Functionality Device
FLiRS	Frequently Listening Routing Slave
FSK	Frequency-shift keying
GSM	Global System for Mobile
HDR	High Dynamic Range
HVAC	Heating, ventilation, and air conditioning
ID	IDentification
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Science and Medical
ITU	International Telecommunication Union
MAC	Media Access Control
NIF	Node Information Frame
NXP	Next eXPerience
OQPSK	Offset quadrature phase-shift keying
PAN	Personal Area Network
PHY	Physical layer
RF4CE	Radio Frequency for Consumer Electronics
RFD	Reduced-Functionality device
S2	Security 2
TLS	Transport Layer Security
WPAN	Wireless Personal Area Network
ZDO	ZigBee Device Object