Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

DIPLOMOVÁ PRÁCE

Internet věcí a monitoring pohybu osob

Bc. David Mašata

© 2023 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. David Mašata

Informatika

Název práce

Internet věcí a monitoring pohybu osob

Název anglicky

Internet Things and Monitoring the Movement of People

Cíle práce

Diplomová práce je tematicky zaměřena na problematiku monitoringu obsazenosti budov s využitím zařízení internetu věci.
Hlavním cílem práce je rozšířit a zpřesnit stávající systém monitoringu obsazenosti o komponenty internetu věcí.
Dílčí cíle práce jsou:
- analyzovat a charakterizovat stávající řešení,
- vybrat vhodné zařízení pro zpřesnění sbíraných pozičních dat,
- implementovat vybrané řešení do stávajícího systému,
- zhodnotit přínosy nového řešení.

Metodika

Teoretická část diplomové práce se bude zakládat na analýze a řešení odborných zdrojů.

V praktické části bude analyzován stávající sytém pro monitoring obsazenosti budov a formulovány jeho nedostatky.

Na základě poznatků z teoretické části a zjištěných nedostatků stávajícího řešení budou na základě vybraných kritérií vybrány vhodné HW a SW nástroje pro zpřesnění získaných dat. Následně sestaven HW a SW IoT prototyp.

Na závěr budou zhodnocena naměřená data a zhodnocen přínos nového opatření.

Na základě syntézy teoretických poznatků a výsledků praktické časti budou formulovány závěry práce.

Doporučený rozsah práce

60–80 stran

Klíčová slova

IoT, internet věcí, chytrá zařízení, lokalizace, bezdrátové sítě, WiFi, Bluetooth, virtuální závory, Arduino, PHP, MySQL, monitoring osob.

Doporučené zdroje informací

APRAJITA, Krishna a Ajit SINGH. Internet of Things & Wireless Sensor Network. 2019. ISBN 1694912388.

COLBACH, Gordon. Wireless Networking: Introduction to Bluetooth and Wifi. Penguin Random House South Afr, 2017. ISBN 9781973252115.

KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

LI, Yan, Johan BARTHELEMY, Shuai SUN, Pascal PEREZ a Bill MORAN. A Case Study of WiFi Sniffing Performance Evaluation. IEEE Access [online]. 2020, 8, 129224-129235 [cit. 2021-6-23]. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2020.3008533

VATTAPPARAMBAN, Edwin, Bekir Sait CIFTLER, Ismail GUVENC, Kemal AKKAYA a Abdullah KADRI. Indoor occupancy tracking in smart buildings using passive sniffing of probe requests. In: 2016 IEEE International Conference on Communications Workshops (ICC) [online]. IEEE, 2016, 2016, s. 38-44 [cit. 2021-6-23]. ISBN 978-1-5090-0448-5. Dostupné z: doi:10.1109/ICCW.2016.7503761

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Michal Stočes, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 27. 9. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 28. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 21. 03. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Internet věcí a monitoring pohybu osob“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 25.03.2023 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Michalu Stočesovi, Ph.D. za profesionální vedení, věcné a cenné rady, jeho přístup a poskytnuté konzultace během psaní diplomové práce. Zároveň bych chtěl poděkovat své rodině, přítelkyni a přátelům za projevenou podporu a poskytnutí vhodných studijních podmínek během celého magisterského studia.

Internet věcí a monitoring pohybu osob

Abstrakt:

Diplomová práce je tematicky rozdělena na dvě základní části. Jedná se o literární rešerše a vlastní práci. První část obsahuje literární rešerše, které představují teoretický úvod do využití chytrých zařízení internetu věcí. Konkrétně je zaměřena na problematiku monitoringu pohybu osob uvnitř budov s využitím zařízení internetu věci. Tato teoretická část je zde především pro pochopení problematiky vlastní práce (druhé části). Literární rešerše jsou neodmyslitelnou součástí každé bakalářské či diplomové práce a jsou hrubou teorií, která je zpracována na základě nastudované literatury k danému tématu.

Druhou částí diplomové práce je vlastní práce. Tato část je obsahově rozdělena do 5 tematických okruhů, které obsahují analýzu stávajícího řešení, návrh nového HW prototypu, softwarové řešení, vizualizace dat a testování. Na základě analýzy byly navrženy vhodné možnosti rozšíření stávajícího řešení, které by měly vést k efektivnějšímu měření. V následujících krocích byl navržen a sestrojen nový HW prototyp, vytvořen potřebný software a vizualizována naměřená data. V poslední řadě bylo vše řádně testováno, aby se předešlo případným chybám či nefunkčním prvkům práce.

Klíčová slova: IoT, internet věcí, chytrá zařízení, lokalizace, bezdrátové sítě, WiFi, Bluetooth, virtuální závory, Arduino, PHP, MySQL, monitoring osob

Internet Things and Monitoring the Movement of People

Abstract:

The thesis is thematically divided into two basic parts. These are the literature research and the thesis itself. The first part contains the literature research, which presents a theoretical introduction to the use of smart IoT devices. Specifically, it focuses on the issue of monitoring the movement of people inside buildings using IoT devices. This theoretical part is mainly there to understand the issues of the actual thesis (second part). Literature searches are an essential part of any bachelor or master thesis and are rough theory that is elaborated based on the studied literature on the topic.

The second part of the thesis is the thesis itself. This part is divided into 5 thematic areas which include analysis of the existing solution, design of a new HW prototype, software solution, data visualization and testing. Based on the analysis, suitable options for extending the existing solution have been proposed, which should lead to more effective measurement. In the following steps, a new HW prototype was designed and built, the necessary software was developed and the measured data was visualized. In the last step, everything was properly tested to avoid possible errors or non-functional elements of the work.

Keywords: IoT, internet of things, smart devices, localization, wireless networks, WiFi, Bluetooth, virtual barriers, Arduino, PHP, MySQL, people monitoring

Obsah

1. ÚVOD 11

2. CÍL A METODIKA PRÁCE 12

2.1. CÍL PRÁCE 12

2.2. METODIKA PRÁCE 12

3. LITERÁRNÍ REŠERŠE 14

3.1. INTERNET VĚCÍ 14

3.1.1. HISTORIE IOT 15

3.1.2. OBLASTI VYUŽITÍ 15

3.1.3. PŘEDPOKLÁDANÝ VÝVOJ IOT 16

3.2. IOT KOMUNIKAČNÍ PROTOKOLY 17

3.2.1. IPV6 17

3.2.2. ZIGBEE 18

3.2.3. BLUETOOTH LOW ENERGY 19

3.2.4. Z-WAVE 19

3.2.5. NFC 20

3.3. LOKALIZACE 20

3.3.1. VNĚJŠÍ LOKALIZACE 21

3.3.2. VNITŘNÍ LOKALIZACE 23

3.3.3. APLIKAČNÍ POŽADAVKY PRO LOKALIZACI 24

3.4. TECHNIKY LOKALIZACE 24

3.4.1. TRIANGULACE 24

3.4.2. PROXIMITY 25

3.4.3. TRILATERACE 26

3.5. MONITORING BUDOV A MÍSTNOSTÍ 28

3.5.1. GDPR 30

3.6. ZPŮSOBY MONITORINGU OSOB UVNITŘ BUDOV 30

3.6.1. WIFI 30

3.6.2. BLUETOOTH 32
3.6.3. KAMEROVÝ SYSTÉM 34
3.7. IOT ČIDLA A SENZORY 34
3.7.1. VIRTUÁLNÍ ZÁVORY 35
3.7.2. SENZOR MNOŽSTVÍ CO_2 40
3.7.3. SENZOR TEPLOTY 40
3.7.4. SENZOR DETEKCE POHYBU 41
3.8. PROGRAMOVACÍ JAZYKY 41
3.8.1. ZNAČKOVACÍ JAZYK HTML 42
3.8.2. KASKÁDOVÉ STYLY CSS 42
3.8.3. SKRIPTOVACÍ JAZYK PHP 43
3.8.4. ARDUINO IDE 43
3.9. IEEE 802.11 44
3.9.1. ARCHITEKTURA WLAN 45
3.9.2. ZABEZPEČENÍ WLAN 46
3.10. DATABÁZOVÝ SYSTÉM MYSQL 46
4. VLASTNÍ PRÁCE 48
4.1. ANALÝZA STÁVAJÍCÍHO ŘEŠENÍ 48
4.1.1. MONITOROVACÍ SYSTÉM WOLNO 49
4.1.2. VYUŽITÍ INTERNETU VĚCÍ PRO MONITORING OBSAZENOSTI BUDOV 50
4.2. NÁVRH HARDWARE PROTOTYPU 51
4.2.1. ŘÍDÍCÍ DESKA WEMOS D1 MINI 52
4.2.2. PAPRSKOVÉ SENZORY 53
4.2.3. BATERIE 9 V (NAPÁJENÍ) 55
4.3. SOFTWAROVÉ ŘEŠENÍ 56
4.3.1. WEBOVÁ APLIKACE 56
4.3.2. ARDUINO WEBOVÝ EDITOR 61
4.3.3. DATABÁZOVÝ PROSTŘEDÍ 65
4.4. VIZUALIZACE DAT 66

4.5. TESTOVÁNÍ 67

5. VÝSLEDKY A DISKUSE 70

5.1. VÝSLEDNÝ PROTOTYP 70

5.1.1. CENOVÝ ROZPOČET MATERIÁLU 71

5.2. MOŽNOSTI BUDOUCÍHO VÝVOJE MONITORINGU BUDOV 72

6. ZÁVĚR 73

7. SEZNAM POUŽITÝCH ZDROJŮ 75

8. SEZNAM OBRÁZKŮ, TABULEK A ZKRATEK 79

8.1. SEZNAM OBRÁZKŮ 79

8.2. SEZNAM TABULEK 80

8.3. SEZNAM ZKRATEK 80

1. Úvod

Začátkem 21. století došlo k vývoji digitálních technologií a informačního věku, což přineslo zásadní změny v oblasti komunikace, zábavy, obchodu, vzdělání a v mnoha dalších oblastech. Je to éra významných změn a pokroků technologií a vývoje společnosti jako celku. Celkově lze říci, že 21. století je érou rychlého technologického a společenského vývoje, který přináší nové výzvy, ale také příležitosti pro celou společnost.

Jedním z nejvýraznějších trendů v oblasti technologií v 21. století se stal internet věcí (IoT). V průběhu 21. století došlo k rapidnímu rozvoji IoT technologií. V prvních letech století byly IoT aplikace především v průmyslu, kde se využívaly k automatizaci a optimalizaci výrobních procesů. Postupem času se však IoT technologie staly dostupnější a začaly se využívat také v domácnostech a dalších oblastech. Jedním z příkladů může být právě monitorování budov.

Díky velmi rychlému rozvoji IoT prvků, jako jsou různé typy senzorů, čidel nebo kamer se internet věcí rozšířil i do firem, institucí a podniků všech velikostí. Je proto logickým krokem tyto prvky využít pro monitorování svých budov a místností, a to za účelem zvýšení zabezpečení, úspory energie a financí nebo pouze za účelem zlepšení zákaznické zkušenosti. Získaná data z budov lze dále využívat například pro optimalizaci nastavení systémů vytápění, klimatizace, cirkulace vzduchu či osvětlení. Benefitem těchto komplexních řešení je vyloučení lidského faktoru a vysoká úspora času a peněz na zaměstnance, kteří by dané činnosti měli zastávat. Zároveň lze díky monitorovacím systémům předcházet přetěžování vnitřních prostor. Na základě těchto získaných dat mohou být prováděny různé typy analýz vedoucí k efektivnějšímu využití daných prostorů a dalších činností či nákladů s nimi spojenými.

Možnosti monitorování vnitřních prostor budov je velmi početné množství, a ještě více pohledů, jak naměřená data sledovat. Důležité je vždy správně definovat, co by mělo být cílem monitorování, za jakým účelem ho provádět a nastavit reálná očekávání.

2. Cíl a metodika práce

2.1. Cíl práce

Diplomová práce se obecně zaměřuje na využití chytrých zařízení internetu věcí. Konkrétně je tematicky zaměřena na problematiku monitoringu pohybu osob uvnitř budov s využitím zařízení internetu věci. Hlavním cílem práce je rozšířit a zpřesnit stávající systém monitoringu osob o komponenty internetu věcí.

Dílčí cíle diplomové práce jsou:

- analyzovat a charakterizovat stávající řešení,
- vybrat vhodné zařízení pro zpřesnění sbíraných pozičních dat,
- implementovat vybrané řešení do stávajícího systému,
- zhodnotit přínosy nového řešení.

2.2. Metodika práce

Diplomová práce je tematicky rozdělena do dvou základních částí. Těmito částmi jsou literární rešerše a vlastní práce. První část obsahuje literární rešerše, které představují teoretický úvod do světa internetu věcí (IoT), jeho následného využití a problematiky IoT jako takové. Tato teoretická část je zde především pro pochopení vlastní práce (druhé části). Literární rešerše jsou neodmyslitelnou částí každé bakalářské či diplomové práce a jsou hrubou teorií, která je zpracována nastudováním dostupné literatury k danému tématu.

Druhou částí práce je vlastní práce, tedy část obsahující metody a analýzy zvolené autorem diplomové práce. Součástí je zpracování HW zařízení (prototyp), které bude zajišťovat sběr dat a SW řešení, to získaná data zpracuje a dále interpretuje tak, aby byla co nejvíce srozumitelná a člověku dobře čitelná.

Rovněž je důležité zmínit, že tato diplomová práce je volně navazující na diplomovou práci Ing. Jana Poláčka na téma „Využití internetu věcí pro monitoring obsazenosti budov“ z roku 2022. Cílem je na tuto práci navázat, zhodnotit a rozšířit o vhodné funkcionality.

Na základě nastudovaných poznatků z literárních rešerší a naměřených výsledků v části vlastní práce bude zpracován závěr diplomové práce, kde budou zhodnoceny a formulovány všechny výsledky a problémy, které během zpracovávání nastaly.

3. Literární rešerše

Tato část diplomové práce je zaměřena na teoretická východiska. V následujících podkapitolách je podrobněji zpracována problematika světa IoT a jeho využití pro monitorování obsazenosti budov či místností. Jsou zde uvedeny i některé příklady technologií a metod monitoringu pomocí chytrý zařízení internetu věcí.

3.1. Internet věcí

Internet věcí (Internet of Things, IoT) je síť fyzických zařízení, která jsou navzájem propojena a schopna mezi sebou komunikovat (přenášet data a informace). Tato zařízení jsou vybavena čipy, senzory a ostatními technologiemi, které jim umožňují přenášet a přijímat data. IoT se skládá z mnoha různých zařízení, jako jsou chytré domácnosti, chytré čipy, senzory, lékařské zařízení atd.

Jednou z hlavních výhod IoT je schopnost propojovat různá zařízení a systémy, což umožňuje automatizaci a řízení procesů. Například chytrý termostat může automaticky regulovat teplotu v domě na základě dat o počasí nebo na základě toho, zda je někdo doma nebo ne. Chytré zavlažování může automaticky řídit zavlažování zahrady na základě dat o počasí a zemědělských podmínkách a mnoho dalšího.

IoT má také mnoho aplikací v průmyslu, příkladem je řízení výroby, zlepšování bezpečnosti a efektivity v dopravě a logistice a v mnoha dalších oblastech. IoT může být rovněž použito k monitorování zdravotního stavu zařízení v průmyslu, což může pomoci předcházet výrobním poruchám a zastavení výroby.

IoT vyžaduje velké množství technologií a standardů, jako je bezdrátové připojení, cloudové služby, big data a analytika, aby mohlo fungovat správně. Vývoj a používání IoT vyžaduje spolupráci mezi mnoha různými společnostmi a organizacemi, včetně výrobců zařízení, poskytovatelů cloudových služeb nebo vývojářů aplikací.

3.1.1. Historie IoT

Jednoduše řečeno, internet věcí se skládá z jakéhokoli zařízení s vypínačem, které je připojeno k internetu. IoT zahrnuje stroje komunikující informace přes internet. Stroje zajišťují přímou komunikaci od doby, kdy byl ve 30. a 40. letech 19. století vyvinut telegraf (první pevná linka). První rádiový přenos hlasu, popisovaný jako „bezdrátová telegrafie“, se uskutečnil 3. června 1900 a poskytl nezbytnou součást pro rozvoj internetu věcí. Vývoj počítačů začal v 50. letech 20. století [1].

Internet, který je sám o sobě významnou součástí internetu věcí, začal jako součást DARPA (Agentura pro obranné pokročilé výzkumné projekty) v roce 1962 a vyvinul se v ARPANET v roce 1969. V 80. letech 20. století začali komerční poskytovatelé služeb podporovat veřejné používání ARPANETu, což mu umožnilo vyvinout se do našeho moderního internetu. Satelity a pevné linky poskytují základní komunikaci pro většinu IoT [1].

GPS se stal skutečností na začátku roku 1993, přičemž ministerstvo obrany poskytlo stabilní, vysoce funkční systém 24 satelitů. To bylo rychle následováno soukromými komerčními satelity, které byly umístěny na oběžnou dráhu, díky čemuž byl IoT mnohem funkčnější [1].

3.1.2. Oblasti využití

Připojování věcí k internetu přineslo revoluci do celého světa. Stroje se díky IoT staly chytřejšími, což umožňuje vytvářet větší hodnotu napříč nejrůznějšími odvětvími [2].

Zemědělský průmysl byl vždy velmi vnímavý k technickým inovacím. S přijetím IoT technologií do tohoto průmyslu je zemědělství stále efektivnější. Pomocí IoT je možné realizovat tzv. precizní zemědělství, které je v dnešní době už velmi rozšířené. Další odvětví, které mohou pomocí IoT maximalizovat svou činnost jsou energetika, finance, zdravotnictví, výrobní procesy, doprava a logistika [2].

IoT poskytuje velmi užitečné informace o shromážděných datech a pomáhá tak v daných odvětvích převážně v následujících aspektech [2]:

- úspora nákladů a zvýšená ziskovost,
- zefektivnění cestování,
- vylepšený provozní výkon,
- snížená spotřeba energie a přetížení,
- větší bezpečnost,
- zajišťuje viditelnost v reálném čase,
- správa skladu.

3.1.3. Předpokládaný vývoj IoT

Internet věcí se v posledních letech rozvíjí velmi rychle a je pravděpodobné, že tento trend bude pokračovat i v následujících letech. Očekává se, že počet připojených zařízení k internetu bude stále výrazně růst, což povede k vytvoření nových možností jak pro společnost, tak pro jednotlivce. IoT se může uplatnit v mnoha oblastech, včetně inteligentních budov a měst, automobilového průmyslu, zdravotnictví a vzdělávání. Kromě toho se očekává, že IoT bude hrát významnou roli při řešení globálních problémů, jako je změna klimatu a šetření zdrojů.

V následujících letech by mělo dojít k dalšímu zlepšení technologií, jako je například síť 5G, která umožní rychlejší a spolehlivější připojení pro zařízení v rámci IoT. Toto povede k většímu využití IoT ve službách pro zákazníky, jako jsou automatické ovládání domácnosti nebo inteligentní měření spotřeby energie. Kromě toho se očekává, že se objeví nové aplikace pro IoT, které usnadní práci a zlepší kvalitu života lidí.

V neposlední řadě bude důležité zajistit bezpečnost a soukromí při používání zařízení v rámci IoT. Očekává se, že se budou vyvíjet nové bezpečnostní technologie a postupy, které budou chránit před útoky hackery a zabrání neoprávněnému získávání osobních údajů.

3.2. IoT komunikační protokoly

Internet věcí (IoT) se skládá z chytrých zařízení, která spolu komunikují. Umožňuje těmto zařízením shromažďovat a vyměňovat si navzájem data. Chytrá zařízení mohou mít kabelová nebo bezdrátová připojení. Pokud jde o bezdrátový IoT, lze k připojení chytrého zařízení použít mnoho různých bezdrátových komunikačních technologií a protokolů, jako je internetový protokol verze 6 (IPv6), přes bezdrátové osobní sítě s nízkým výkonem, ZigBee, Bluetooth Low Energy (BLE), Z-Wave a Near Field Communication (NFC). Jedná se o standardní síťové protokoly krátkého dosahu. Následující část této kapitoly bude věnována porozumění různým komunikačním protokolům v IoT [3].

3.2.1. IPv6

Internetový protokol verze 6 (IPv6) je nejnovější verze internetového protokolu vytvořená skupinou IETF (Internet Engineering Task Force), která pomáhá identifikovat a lokalizovat koncové systémy v počítačové síti a směrovat online provoz. Zároveň řeší problém vyčerpání adres IPv4 v důsledku dlouhodobého používání internetu po celém světě [4].

IPv6 je protokol síťové vrstvy, který umožňuje komunikaci po síti. Každé zařízení na internetu má jedinečnou IP adresu, která slouží k jeho identifikaci a zjištění, kde se nachází. V době digitální revoluce v 90. letech 20. století bylo zřejmé, že IP adresy, které internetový protokol verze 4 (IPv4) používal k propojení zařízení, nebudou stačit poptávce. Proto se IETF pustila do vývoje internetového protokolu nové generace. Protokol IPv6 se stal v prosinci 1998 návrhem standardu IETF a 14. července 2017 byl schválen jako internetový standard pro celosvětové zavedení [3].

Adresy IPv4 se vyčerpávaly v důsledku rychlého růstu počtu uživatelů internetu, četného využívání zařízení, jako jsou mobilní telefony, notebooky a počítače, neefektivního využívání adres a neustále zapnutých zařízení, jako jsou kabelové modemy. Pro zmírnění problému vyčerpání adres v protokolu IPv4 byly vyvinuty technologie, jako jsou třídní sítě, beztřídní směrování mezi doménami a překlad síťových adres. Tyto technologie přispěly k

řešení tím, že zavedly zlepšení v páteřních systémech přidělování adres a směrování v síti [3].

Paket IPv6 je sestaven ze 40 rozšířených oktetů, takže uživatelé mohou protokol do budoucna škálovat, aniž by narušili jeho základní strukturu. Paket má dvě části: záhlaví a zápatí [4].

3.2.2. ZigBee

Protokol ZigBee nebo také ZigBee/IEEE 802.15.4 je specifický protokol vytvořený primárně pro bezdrátové sítě. Zahrnuje standardní návrh hardwaru a softwaru pro bezdrátové senzorové sítě vyžadující vysokou spolehlivost, nízké náklady, nízkou spotřebu, škálovatelnost a nízkou rychlost přenosu dat [5].

Bezdrátové senzorové sítě (Wireless Sensor Network, WSN) se skládají z levných bezdrátových senzorů, které jsou schopny shromažďovat, ukládat a zpracovávat informace o prostředí a komunikovat se sousedními uzly. Například v domácnostech lze WSN použít k řízení osvětlení, vytápění, větrání, klimatizaci, monitorování bezpečnosti a detekci mimořádných událostí [5].

ZigBee poskytuje velmi nízkou spotřebu a účinnost díky přizpůsobitelnému pracovnímu cyklu, nízkým rychlostem a nízkému pokrytí rádia. Umožňuje rozsáhlé sítě pro WPN, což z něj činí jeden z nejvhodnějších standardů pro tento účel [5].

Standard	ZigBee/IEEE 802.15.4	Bluetooth	UWB	IEEE 802.11 b/g
Working frequency	868/915 MHz, 2.4GHz	2.4 GHz	3.1 - 10.6 GHz	2.4 GHz
Range (m)	30 – 75+	10 – 30	~10	30 – 100 +
Data rate	20/40/250 kbps	1 Mbps	100+ Mbps	2 – 54 Mbps
Devices	255 – 65k	8		50 – 200
Power consumption	~1 mW	~40 – 100 mW	~80 – 300 mW	~160 mW – 600W
Cost ($US)	~2 – 5	~4 – 5	~5 – 10	~20 – 50

Obrázek 1 - Přehled vlastností ZigBee oproti jiným protokolům

Použití protokolu ZigBee má v porovnání s jinými protokoly pro WSN několik výhod. Jednou z hlavních výhod je, že protokol ZigBee je standardizován na všech vrstvách, což zajišťuje vzájemnou kompatibilitu produktů různých výrobců. Další výhodou je síla sítě. Zařízení mají tendenci se spojovat s každým blízkým zařízením, což umožňuje, aby každý uzel sítě byl dosažitelný z každého jiného uzlu a rozšiřoval tak síť. ZigBee také obsahuje tzv. samoléčebný systém. Pokud preferovaná cesta k uzlu selže, existují další cesty, jak se k uzlu dostat. Čím více zařízení máte, tím je síť spolehlivější [5].

3.2.3. Bluetooth Low Energy

Chování a princip Bluetooth Low Energy (BLE) je dále mírně nastíněn v 3.6.2. Zde jsou popsány detailnější specifikace. BLE je navrženo pro provoz s velmi nízkou spotřebou energie. Přenáší data ve 40 kanálech v nelicencovaném frekvenčním pásmu 2,4 GHz a poskytuje vývojářům obrovskou flexibilitu při vytváření produktů, které splňují jedinečné požadavky na připojení. BLE podporuje více komunikačních topologií, které se rozšiřují z point-to-point sítě na novější mesh topologii. To umožňuje technologii Bluetooth podporovat vytváření spolehlivých rozsáhlých sítí. Ačkoli byl BLE původně známý pro své komunikační schopnosti, je nyní také široce používán jako technologie pro určování polohy zařízení, která reaguje na rostoucí poptávku po službách určování polohy s vysokou přesností uvnitř budov [6].

3.2.4. Z-Wave

Z-Wave je bezdrátový komunikační protokol používaný především v sítích inteligentních domácností, který umožňuje propojení inteligentních zařízení a vzájemnou výměnu řídicích příkazů a dat. Díky obousměrné komunikaci prostřednictvím sítě mesh a potvrzování zpráv pomáhá protokol Z-Wave zmírnit problémy s napájením a přináší do domácí automatizace levné bezdrátové připojení, které nabízí alternativu WiFi s nižší spotřebou energie a alternativu pro Bluetooth s větším dosahem [3].

Z-Wave se skládá z IoT zařízení a primárního řídicího prvku, známého také jako rozbočovač chytré domácnosti, který je jediným zařízením v síti Z-Wave, jež je obvykle připojeno k internetu. Když rozbočovač Z-Wave obdrží příkaz z aplikace chytré domácnosti v chytrém telefonu, tabletu nebo počítači uživatele, přesměruje příkaz do cílového zařízení v síti. Pomocí technologie síťového směrování zdrojů mohou signály Z-Wave přeskakovat přes jiná zařízení Z-Wave, aby se dostaly k zařízení, které chce uživatel ovládat. Každá tato síť Z-Wave umožňuje maximálně čtyři přeskoky [7].

Z hlediska identifikace a autorizace je každá síť Z-Wave identifikována pomocí síťového ID a každé koncové zařízení je identifikováno pomocí ID uzlu. Jedinečné síťové ID zabraňuje například tomu, aby jeden dům vybavený systémem Z-Wave ovládal zařízení v jiném podobně vybaveném domě [7].

3.2.5. NFC

NFC (Near Field Communication) je soubor bezdrátových technologií s krátkým dosahem, které obvykle vyžadují k navázání spojení vzdálenost maximálně 4 cm. NFC umožňuje sdílet malé datové soubory mezi značkou NFC tagu a zařízením taktéž podporující protokol NFC [3].

Tagy mohou být různě složité. Jednoduché tagy nabízejí pouze sémantiku čtení a zápisu, někdy s jednorázově programovatelnými oblastmi, které umožňují, aby karta byla určena pouze pro čtení. Složitější tagy nabízejí matematické operace a mají kryptografický hardware pro ověření přístupu k sektoru. Nejsložitější tagy obsahují operační prostředí, které umožňuje komplexní interakci s kódem prováděným na tagu. Data uložená v tagu mohou být také zapsána v různých formátech [8].

3.3. Lokalizace

Pojmem lokalizace je označován mechanismus pro zjišťování prostorových vztahů mezi objekty. Služby vyžadující polohu ke svému fungování nazýváme služby založené na

poloze (Location Based Services, LBS). Tyto aplikace zadržují geografická data (převážně souřadnice) v reálném čase. K lokalizaci používají technologie ke sledování polohy [9].

Služby založené na poloze integrují data z různých zdrojů, včetně systému GPS, aby poskytovaly služby založené na geografické poloze uživatele. Přestože technologie založené na poloze jsou komerčně dostupné již téměř dvě desetiletí, aplikace a služby využívající geodata se v poslední době staly hlavním proudem, a to díky rozšířenému používání chytrých telefonů a tabletů [10].

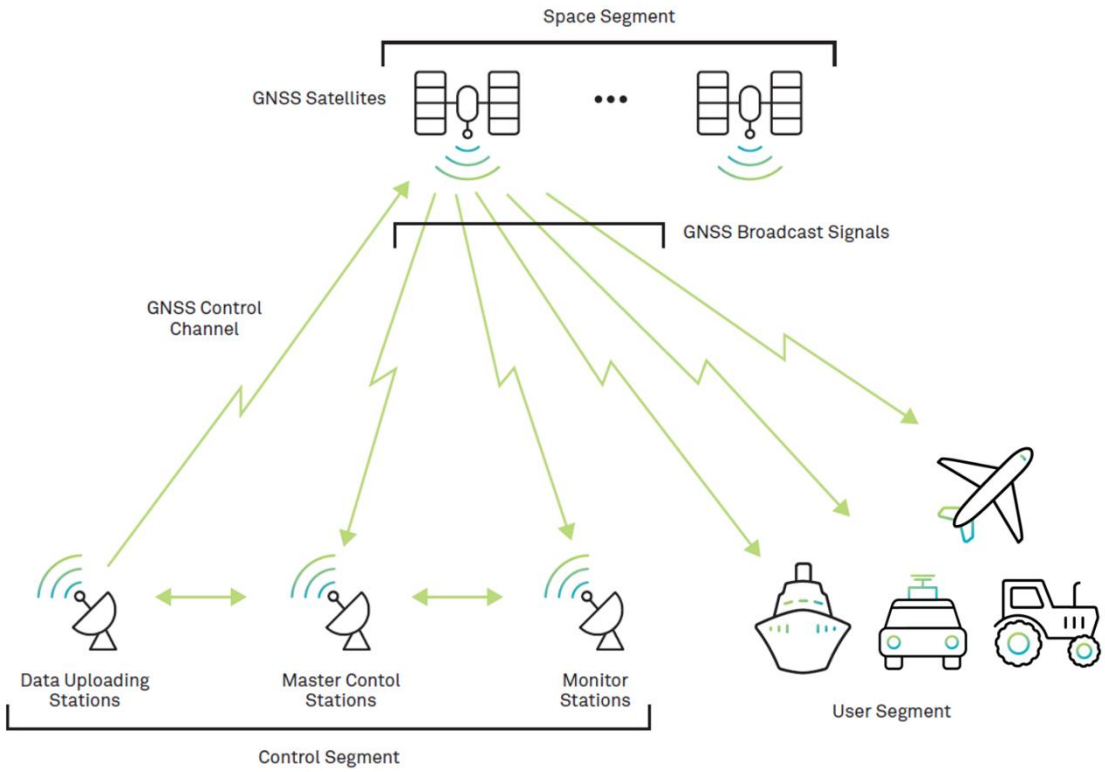
I když existují jasné výhody a relevantní případy použití pro služby založené na poloze, existují určitá rizika, na která je nutné dbát. V minulosti byli tvůrci aplikací, vývojáři mobilních zařízení a operátoři mobilních sítí obviňováni ze sledování zařízení u uživatelů bez jejich souhlasu. Údaje o sledování polohy ve špatných rukou mohou vést k nebezpečným situacím, k odcizení soukromých informací nebo v menším měřítku mohou být data použita pro nevyžádané cílené marketingové nebo reklamní kampaně, které mohou být při nejmenším velmi otravné [10].

3.3.1. Vnější lokalizace

Globální polohový systém (Global Positioning System, GPS) řadíme mezi vnější lokalizace. Jedná se o konstelaci družic, která podporuje vysoce přesná měření polohy, navigace a času po celém světě. Jako jeden z prvních družicových systémů určování polohy se GPS stal nedílnou součástí prací prováděných po celém světě, včetně přesného zemědělství, autonomních vozidel, námořního nebo leteckého průmyslu. GPS je jedním z mnoha globálních navigačních satelitních systémů (Global Navigation Satellite Systems, GNSS), které poskytují měření polohy, navigace a času. Systém GPS provozují americké vesmírné síly, součást amerických ozbrojených sil, ale může jej používat kdokoli na celém světě [11].

Systém GPS byl spuštěn v roce 1973 a první družice byla vypuštěna v roce 1978. Družice jsou vyvíjeny a vypouštěny v sériích známých jako bloky. V letech 1978-1981 bylo

vypuštěno celkem 10 družic (blok 1). Družice druhé řady (blok 2) byly vypuštěny počínaje rokem 1989 a byly schopny vysílat na dvou rádiových frekvencích v jednom pásmu [11].



Obrázek 2 - Schéma architektury GNSS

GPS zahrnuje tři hlavní segmenty:

- vesmírný segment,
- řídicí segment,
- uživatelský segment.

Vesmírný segment GPS zahrnuje více než 30 družic na oběžné dráze, které provozují a udržují americké vesmírné síly. Tyto družice vysílají rádiové signály do řídicích a monitorovacích stanic na Zemi a zároveň uživatelům, kteří vyžadují vysoce přesné určení polohy [11].

Americké vesmírné síly rovněž dohlížejí na řídicí segment GPS. Ten zahrnuje hlavní řídicí a záložní řídicí stanice, vyhrazené pozemní antény a několik monitorovacích stanic

rozmístěných po celém světě. Tyto stanice se starají o to, aby družice GPS byly zdravé, obíhaly ve správných polohách a měly na palubě přesné atomové hodiny. Tyto stanice jsou nedílnou součástí celkového stavu a přesnosti konstelace GPS [11].

Uživatelský segment zahrnuje všechny, kteří se spoléhají na družice GPS při měření. Od mobilního telefonu poskytujícího pokyny až po autonomní vozidla vyžadující přesnost určení polohy na úrovni jízdního pruhu [11].

3.3.2. Vnitřní lokalizace

Rozšíření bezdrátových lokalizačních technologií představuje slibnou budoucnost pro monitorování osob ve vnitřních prostorách. Jejich aplikace zahrnují mimo jiné sledování v reálném čase, rozpoznávání aktivit aj. Vnitřní lokalizační technologie navíc řeší neefektivitu GPS uvnitř budov. Vzhledem k tomu, že lidé tráví většinu svého času ve vnitřním prostředí, je služba sledování uvnitř budov veřejností velmi žádaná. Pro tyto účely je zde uveden přehled stávajících lokalizačních technologií, které lze použít pro sledování osob ve vnitřním prostředí [12].

Vnitřní lokalizaci lze dále členit na absolutní a sektorovou. Za účelem monitorování osob uvnitř budov není vždy striktně nutné znát přesnou polohu sledovaných osob. Mnohdy postačí znát například pouze místnost, patro, sektor, kde se daná osoba v rámci budovy nachází.

Při absolutní lokalizaci dochází k měření polohy s přesností závisející na velikosti odchylky. Jedná se sice o přesnější lokalizaci, ale zároveň také o technicky velmi náročnou. V případech, kdy není nezbytně nutné použít absolutní lokalizaci se velmi často využívá naopak lokalizace sektorové. Ta na rozdíl od absolutní není tak technicky náročná a tím pádem i levnější. Sektorová lokalizace určuje pouze jistou oblast, kde se sledovaný nachází. Často tedy postačí v rámci objektu lokalizovat pouze místnost, patro nebo oblast výskytu osoby. Sektorová lokalizace zachycuje také dlouhodobější a globálnější polohu monitorovaných osob [12].

3.3.3. Aplikační požadavky pro lokalizaci

Měřítko a přesnost – hodnoty vyjadřují jaké jsou nejmenší měřitelné vzdálenosti, v jakém prostoru je možné je měřit a jaká je jejich odchylka od skutečnosti. Například souřadnicový systém GPS bude mít měřítko s přesností kolem jednoho metru v závislosti na přesnosti vnitřních hodin a kvalitě signálu z družic [9].

Dynamika – určuje, zda jsou senzory pohyblivé, nebo statické, případně jak často by měla být prováděna kalibrace senzorů [9].

Hustota senzorové sítě – určuje, jak daleko od sebe by měly být senzory rozmístěny, nebo také kolik sousedů by měl každý senzor mít ve svém rádiovém dosahu [9].

Energetické a komunikační schéma – popisuje princip úspory elektrické energie a s ním související komunikační schéma systému. To zahrnuje například způsob přenosu dat od uzlů do základnové stanice (využití a způsob agregace dat) nebo naopak přenos řídících dat ze základnové stanice k cílovým uzlům v senzorové síti. Nebo také představa o spouštění procesu lokalizace [9].

Prostředí – prezentuje vlastnosti prostředí, ve kterém má být senzor lokalizován (uvnitř budov, venkovní, pod vodou, pod zemí). Každé prostředí pro lokalizaci přináší unikátní výzvy. Například systémy uvnitř budov by měly počítat s odlišnými faktory než systém venkovní lokalizace, který musí brát ohled například na proměnlivost počasí [9].

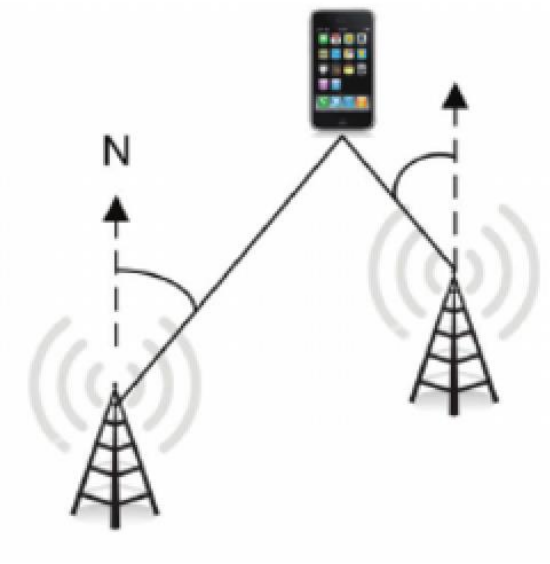
3.4. Techniky lokalizace

3.4.1. Triangulace

Triangulace je způsob, jak určit polohu něčeho pomocí polohy jiných věcí. Běžně ji používají například geologové k určení polohy zemětřesení nebo se používá k určení polohy kosmických objektů. Existuje několik způsobů, jak triangulaci použít k určení polohy.

Pro úspěšnou triangulaci musíte být schopni vidět v terénu prvky nebo orientační body a identifikovat je na mapě. Z tohoto důvodu je použití této techniky za snížené

viditelnosti obtížné. Nicméně ve všech případech (i za tmy) by mělo být možné vyčlenit alespoň několik použitelných orientačních bodů nebo prvků v okolí. Mezi nápadnější nebo zjevné prvky, které můžete použít, patří budovy, vrcholy, kopce, balvany, srázy, jezera, rybníky nebo skalní výchozy [13].



Obrázek 3 - Schéma triangulace

3.4.2. Proximity

Aby bylo možné plně využít potenciál znalosti polohy a umožnit nové pokročilé služby založené na poloze, je třeba lokalizační algoritmy kombinovat s doplňkovými technologiemi, včetně přesného odhadu výšky, tj. trojrozměrné polohy, dále pak spolehlivé klasifikace mobility uživatelů a účinných řešení pro mapování uvnitř budov. Tento přehled poskytuje ucelený přehled těchto podpůrných technologií [14].

Lokalizace pomocí měření blízkosti je oblíbená, když nízké náklady mají přednost před přesností. Měření blízkosti jednoduše hlásí, zda jsou dvě zařízení spojena nebo alespoň v dosahu. Termín "proximity" však může vést k omylu, že blízkost je čistě geometrická funkce. Tedy zda jsou dvě zařízení od sebe vzdálena méně než určitou vzdálenost nutnou pro spojení. Ve skutečnosti, je proximita určována pomocí přijímače, který dekóduje paket vyslaný vysílačem [14].

V těchto lokalizačních systémech je poloha určena na základě polohy nejbližšího vysílače. Přesnost lokalizace zde závisí na hustotě sítě vysílačů. V systémech fungujících na tomto principu je prostor rozdělen na segmenty podle poloh jednotlivých vysílačů [15].

Obrázek 4 - Schéma proximity

3.4.3. Trilaterace

Trilaterace je alternativou triangulace, která se opírá pouze o měření vzdálenosti. Díky technologiím měření vzdálenosti je trilaterace nákladově efektivnější technikou určování polohy. Trilaterace se používá mimo jiné i k určování souřadnic polohy pomocí satelitů a přijímačů globálního polohového systému [16].

Obrázek 5 - Schéma trilaterace

Existuje několik trilateračních typů:

- 2D trilaterace,
- 3D trilaterace,
- GSM trilaterace,
- WiFi trilaterace,
- Bluetooth trilaterace,
- zvuková trilaterace.

2D trilaterace – poloha hledaného bodu se určuje ve dvourozměrném prostotu, proto nám známé body a hledaný bod musí být umístěny v jedné rovině. Princip spočívá ve vytvoření kružnic kolem známých bodů s poloměry o velikostech vzdáleností k hledanému bodu. Pokud jsou známé pouze dva body, dochází k průniku kružnic ve dvou místech. Z toho vyplývá, že k přesnému určení polohy hledaného bodu je za potřebí minimálně tří známých bodů [17].

3D trilaterace – princip je stejný jako u 2D trilaterace, jen výpočet a zobrazení je složitější na představu. Body mají souřadnice (x, y, z) a kolem námi známých bodů jsou vytvořeny koule s poloměry o velikostech vzdáleností k hledanému bodu [17].

GSM trilaterace – nejjednodušší a nejméně přesné určení pozice telefonu je pomocí telefonních vysílačů (Base Transceiver Station, BTS). Každý vysílač má svou unikátní identifikaci. Pokud tedy telefon komunikuje s konkrétním vysílačem, je v kruhu, jehož středem je vysílač a poloměr kruhu tvoří dosah vysílače [17].

WiFi trilaterace – firmy jako Google mají rozsáhlé databáze MAC adres jednotlivých AP a k nim přiřazená zeměpisné souřadnice. Díky tomu, pokud je na telefonu zapnutá WiFi, stačí když zjistí MAC adresy zařízení v dosahu a pošle dotaz prostřednictvím internetu. Polohu lze ještě zpřesnit pomocí intenzity signálu [17].

Bluetooth trilaterace – nasazení Bluetooth pro trilateraci se v mnohém shoduje s WiFi. Dokonce operuje i ve stejném pásmu 2,4 GHz. Technologie Bluetooth byla vytvořena pro bezdrátovou komunikaci na krátké vzdálenosti. Hardware potřebný ke komunikaci je tak menší a levnější. Trilaterace Bluetooth funguje na principu komunikace master – slave,

tedy jeden řídící uzel a ostatní uzly vedlejší. Vyhledávání Bluetooth zařízení v okolí navíc trvá dlouho. Tyto verze nejsou vhodné pro časté dotazy na intenzitu signálu [17].

Zvuková trilaterace – stejně jako u Bluetooth nebo WiFi lze využít dobu cesty signálu k výpočtu vzdálenosti. V tomto případě neputuje signál rychlostí světla, ale jedná se o zvukové signály šířící se rychlostí zvuku [17].

3.5. Monitoring budov a místností

Monitorování obsazenosti může být přínosné prakticky pro všechny podniky. Jsou to převážně firemní kancelářské prostory, univerzity, maloobchody, automobilový průmysl nebo pohostinství. Může se jednat o nákladově efektivní způsob, jak zlepšit provoz podniku a zážitky návštěvníků. Tyto údaje o obsazenosti lze využít k získání informací o využití prostor v reálném čase nebo v minulosti [18].

Technologie monitorování obsazenosti, známá také jako počítání osob, monitorování pěšího provozu nebo technologie řízení davu, počítá počet osob, které se právě nacházejí v určité budově, patře nebo jiném definovaném prostoru. Existuje mnoho způsobů, jak monitorovat počet osob v prostoru. Některé způsoby jsou zastaralé a nevyžadují žádnou technologii. Jiné využívají sofistikovaný hardware či algoritmy [18].

Zde je několik různých druhů možností monitorování obsazenosti, které jsou v současné době k dispozici:

- ruční monitorování,
- senzory lomového paprsku,
- tepelné senzory,
- kamerové senzory,
- radarové senzory,
- senzory WiFi a Bluetooth.

Ruční monitorování – jedná se o typ monitorování, kdy typicky zaměstnanec stojí před obchodem a pomocí ručního počítadla sleduje, kolik zákazníků vchází a vychází z obchodu/budovy, aby se ujistil, že nepřekročí kapacitu návštěvníků [18].

Senzory lomového paprsku – ty detekují pohyb pomocí infračervených světelných paprsků, které počítají počet osob na základě toho, kolikrát je čára překročena. Tyto snímače jsou obvykle umístěny na obou stranách dveří, jsou levné a poskytují dobrý základní trend. Jsou však náchylné k chybám a chybí jim granularita konkrétnějších částí budovy, kterými návštěvníci procházejí [18].

Tepelné senzory – tyto senzory detekují tělesné teplo, když osoba prochází kolem senzoru, a tím monitorují obsazenost. Tato technologie je anonymní, nicméně přesnost může být problematická, pokud se lidé nehýbou, překrývají nebo nesou teplé předměty, jako je třeba notebook či horký nápoj [18].

Kamerové senzory – pomocí kamerového systému aktivně počítají počet osob, které vcházejí a vycházejí. Vzhledem k absenci anonymity jsou skvělé pro podniky, které chtějí získat více informací o tom, kdo jsou jejich zákazníci (tj. pohlaví, věk atd.). Kamerové snímače vyžadují k nastavení určité změny v infrastruktuře. Zde je však nutné dbát na dodržení všech náležitostí legislativy GDPR [18].

Radarové senzory – lze instalovat prakticky kdekoli na stropě a detekovat pohyblivé nebo stacionární objekty. Díky svému pozorovacímu bodu mohou pokrýt velké plochy, monitorovat obsazenost a jsou často oblíbené v kancelářských budovách. Přestože pokrývají velkou plochu, mohou při velkém pohybu ztrácet přesnost [18].

Senzory WiFi a Bluetooth – tento přístup využívá snímače, které se obvykle snadno instalují a snímají signály Bluetooth a WiFi (telefony, tablety nebo nositelná zařízení). Zajišťují celkový počet jedinečných signálů v prostoru. Pomocí algoritmů strojového učení se signály analyzují a vypočítá se počet osob v konkrétním prostoru. Pomocí této metody lze monitorovat celou budovu nebo konkrétní patro. Osobní údaje jsou chráněny a zároveň poskytují velmi přesné měření obsazenosti [18].

3.5.1. GDPR

„Obecné nařízení o ochraně osobních údajů (GDPR) je nejpřísnějším zákonem o ochraně osobních údajů a bezpečnosti na světě. Ačkoli bylo navrženo a schváleno Evropskou unií (EU), ukládá povinnosti organizacím kdekoli, pokud se zaměřují na osoby v EU nebo shromažďují údaje o nich. Nařízení vstoupilo v platnost 25. května 2018. GDPR ukládá přísné pokuty těm, kteří poruší jeho normy ochrany osobních údajů a zabezpečení, přičemž sankce dosahují desítek milionů eur.“ [1]

Nařízením GDPR dává Evropa najevo svůj pevný postoj k ochraně osobních údajů a bezpečnosti v době, kdy stále více lidí svěřuje své osobní údaje cloudovým službám a kdy jsou případy narušení bezpečnosti na denním pořádku. Samotné nařízení je rozsáhlé, dalekosáhlé a poměrně málo konkrétní, což z dodržování GDPR činí skličující vyhlídku, zejména pro malé a střední podniky [19].

3.6. Způsoby monitoringu osob uvnitř budov

V této části jsou podrobně popsané nejrozšířenější typy a způsoby, které lze použít pro monitorování osob v rámci vnitřních prostor. Jsou zde prezentovány technické aspekty, jejich přínos či principy použití pro monitoring.

3.6.1. WiFi

Definicí WiFi je myšlena bezdrátová technologie používaná k připojení počítačů, tabletů, smartphonů a dalších zařízení k internetu. WiFi je rádiový signál odeslaný z bezdrátového směrovače do blízkého zařízení, který převádí signál na data, která můžete vidět a používat. Zařízení vysílá rádiový signál zpět do routeru, který se připojuje k internetu drátem nebo kabelem [20].

[1] **GDPR.eu. 2023**. What is GDPR, the EU’s new data protection law? Načteno z *https://gdpr.eu/what-is-gdpr/*

Síť WiFi je jednoduše připojení k internetu, které je sdíleno s více zařízeními v domácnosti nebo ve firmě prostřednictvím bezdrátového směrovače. Router je připojen přímo k vašemu internetovému modemu a funguje jako rozbočovač pro vysílání internetového signálu do všech vašich zařízení podporujících též WiFi. Což přináší značnou flexibilitu – zůstanete připojeni k internetu, dokud jste v oblasti pokrytí sítě [20].

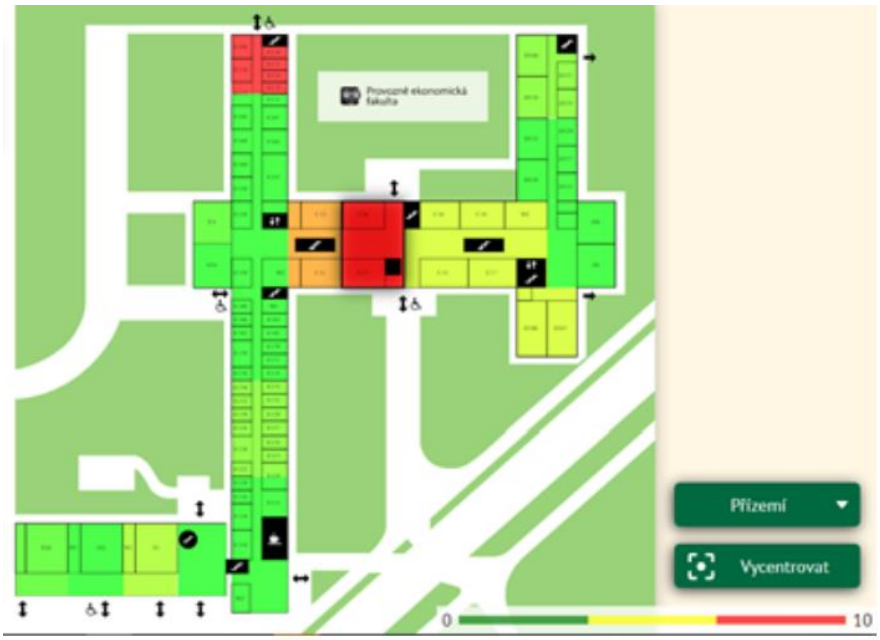
Existuje několik typů, jak se k WiFi lze připojit:

- kabelová linka/router,
- mobilní hotspot,
- LTE domácí internet,
- 5G domácí internet.

Co se týče využití bezdrátové sítě WiFi pro monitoring, tak se jedná o jednu z nepoužívanějších technologií pro lokalizaci osob uvnitř budov. Tato metoda pracuje na principu počítání připojených uživatelů k AP (Access Point). Aby byla tato metoda co nejvíce úspěšná, je nutné mít kvalitně zpracovanou infrastrukturu těchto přístupových bodů v budově.

Na principu této technologie funguje například monitorovací systém WOLNO, který je aktivně používaný na České zemědělské univerzitě v Praze, konkrétně na Provozně ekonomické fakultě. „*Tato aplikace poskytuje informace o obsazenosti oblastí v areálu na základě provozních parametrů bezdrátové infrastruktury univerzitní WiFi sítě. Studenti se díky tomu mohou podívat, kde je aktuálně nejvíce lidí a podle toho si např. vybrat místo, kde budou mít nejvíce klidu pro studium.*“ [2]

[2] **Katedra informačních technologií. 2020**. Obsazenost areálu ČZU. Načteno z *https://ls40.pef.czu.cz/obsazenost-arealu-czu*



Obrázek 6 - Rozhraní aplikace WOLNO

Kromě poskytování údajů související s obsazeností učeben a místností v reálném čase, je zároveň možné v aplikaci filtrovat pouze určitý časový interval z historických dat nebo vytvořit graf průměrné obsazenosti budovy, místnosti nebo učebny v čase. Tyto informace mohou sloužit k další optimalizaci. Příkladem může být chytré vytápění nebo tvorba studentských rozvrhů [21].

Dalším typickým příkladem využití WiFi pro monitorování osob může být Google Geolocation API. To vrací polohu a poloměr přesnosti na základě informací o mobilních zařízeních a uzlech WiFi, které může klient detekovat. Jednotlivá zařízení následně odesílají svá polohová data (skrze GPS nebo GSM) do databází společnosti Google. Databáze díky těmto informacím obsahují data o poloze přístupových bodů WiFi. Pomocí těchto všech dat a informací, lze následně lokalizovat polohu osoby [15].

3.6.2. Bluetooth

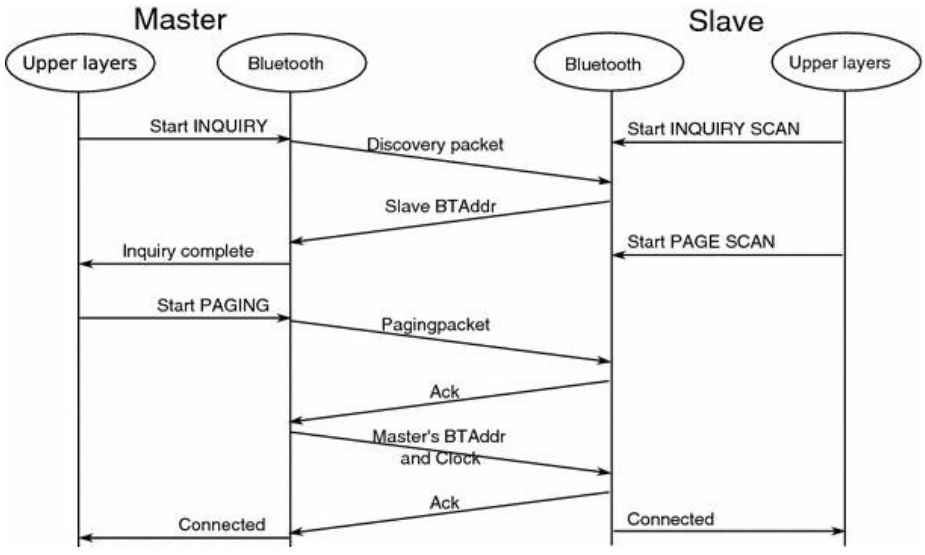
Bluetooth je bezdrátová technologie, která využívá rádiovou frekvenci ke sdílení dat na krátkou vzdálenost, čímž eliminuje potřebu kabelů. Pomocí Bluetooth na svém mobilním

zařízení můžete sdílet dokumenty nebo se připojit k jiným zařízením podporujícím tuto technologii. Z bezpečnostních důvodů musí být zařízení Bluetooth před zahájením přenosu informací spárována. Proces párování vašich zařízení se bude lišit v závislosti na zařízení, ke kterému se připojujete [22].

Jednou z nevýhod Bluetooth je, že spotřebovává poměrně dost baterie z vašeho zařízení. Pokud bude připojení Bluetooth zapnuté celý den, spotřeba energie bude velmi patrná. Z tohoto důvodu byl navržen Bluetooth Low Energy (BLE), který má tento problém pomoci vyřešit [23].

Bluetooth Low Energy je založeno na technologii Bluetooth. Byl vydán v roce 2011 a je také označován jako Bluetooth Smart nebo Bluetooth 4.0. BLE je navrženo tak, aby nabízelo mnoho stejných funkcí jako Bluetooth, ale zaměřuje se na nízkou spotřebu. Díky tomu není tak rychlý jako Bluetooth a nehodí se pro přenos velkých souborů. Je ale ideální pro přenos malého množství dat s minimální spotřebou energie. Tyto parametry BLE jsou naprosto ideální pro IoT zařízení. BLE umožnilo široké řadě malých zařízení IoT, jako jsou senzory a štítky, komunikovat i přes to, že nemají velké baterie [23].

Mnoho z nejpopulárnějších aplikací internetu věcí by nebylo možné bez Bluetooth Low Energy provozovat. Snížením spotřeby energie umožňuje IoT zařízením být výrazně menší a vydržet déle. BLE je proto zodpovědná za mnoho nositelných zařízení, štítků a dalších chytrých zařízení, která dnes používáme [23].



Obrázek 7 - Schéma komunikace BLE

3.6.3. Kamerový systém

Metoda monitorování osob pomocí kamer se v posledních letech velmi rozrostla a zlepšila. Velké zásluhy o nárůst těchto monitorovacích systémů se zasloužila i pandemie covid-19. Mnoho společností, obchodní řetězců, maloobchodů nebo velkých korporátních firem v této době byla nucena zavést nebo zlepšit systém pro počítání osob. Jednou z variant, jak osoby monitorovat či počítat jsou právě kamery.

Kamery lze použít ke sledování pohybu osob s připojeným algoritmem počítadla osob, který dokáže detekovat a zaznamenat, kolik lidí projde zónou počítání. Široké vchody a prostory jsou řešeny propojením několika kamer. Nicméně kamery nejsou primárně určeny pro řešení počítání lidí, což způsobuje omezení a vede k neefektivnímu monitorování a nízké přesnosti. Tato technologie je také ovlivněna překážkami a má tendenci poskytovat špatné výsledky, když se pohybují předměty, jako jsou dětské kočárky nebo stíny. Dalším rizikem může být i fakt, že při použití kamer dochází k snímaní obličejů vstupují osob. To může být problematické z pohledu GDPR, proto je zde kladen vyšší důraz na zabezpečení [25].

Jelikož kamery nejsou navrženy tak, aby počítaly lidi – přesnost je nízká. Pro pokrytí širších vchodů je potřeba nainstalovat více kamer v různých úhlech, což zároveň zvyšuje náklady [25].

3.7. IoT čidla a senzory

Důležitou součástí chytrých IoT řešení jsou totiž bezpečností čidla a senzory. Hrají totiž hlavní roli v chodu celého ekosystému. Na základě těchto čidel jste schopni monitorovat domácnost, budovu či jiný prostor z desítek různých pohledů – požární a záplavová čidla, kamerový systém, senzor UV záření či otevřených oken. Bezpečnostních čidel je opravdu mnoho a je důležité vždy správně rozhodnout, která použít.

V této kapitole si podrobněji seznámíme s některým z nich. Primárně je kapitola zaměřena na senzory vhodné k použití počítání osob. Okrajově se však dotkne i jiných senzorů často používaných v IoT, například v chytrých domácnostech. Počítadla

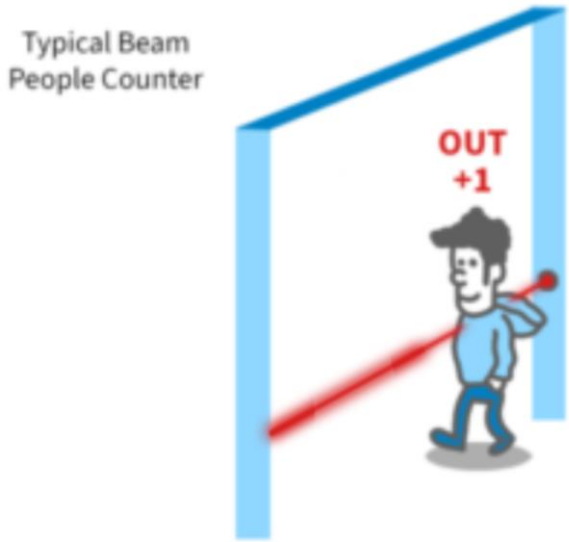
návštěvníků poskytují užitečné údaje o návštěvnosti, které pomáhají manažerům činit chytrá obchodní rozhodnutí. Senzory lze použít v různých průmyslových odvětvích.

3.7.1. Virtuální závory

Virtuální závory představují pro člověka neviditelnou bránu průchodu. Jakmile osoba projde bránou je zaznamenána. Technologií, jak tyto závory použít je hned několik. Nejběžnějšími typy virtuálních závor jsou:

- paprskový senzor,
- teplený senzor,
- Time-of-Flight senzor,
- 2D Mono senzor,
- 3D stereo.

Paprskové senzory neboli také infračervené paprsky se skládají z přijímacích a vysílacích jednotek instalovaných vedle sebe u vchodů. Když je přenosový signál zablokován kvůli překážce objektu, dojde k počítání. Výhodou je levnější varianta pro základní aplikace a také se rychle a snadno instaluje. Naopak tyto senzory mají dvě základní nevýhody. Zaprvé neposkytují čísla vstupů a výstupů odděleně, protože nemají smysl pro směr a zadruhé paprsky nepatří mezi nejpřesnější, protože objekty vedle sebe se počítají jako jeden a zároveň se snižuje přesnost s rostoucí šířkou dveří. Dále pak senzor není schopen filtrovat položky, jako jsou nákupní vozíky nebo dětské kočárky [25].

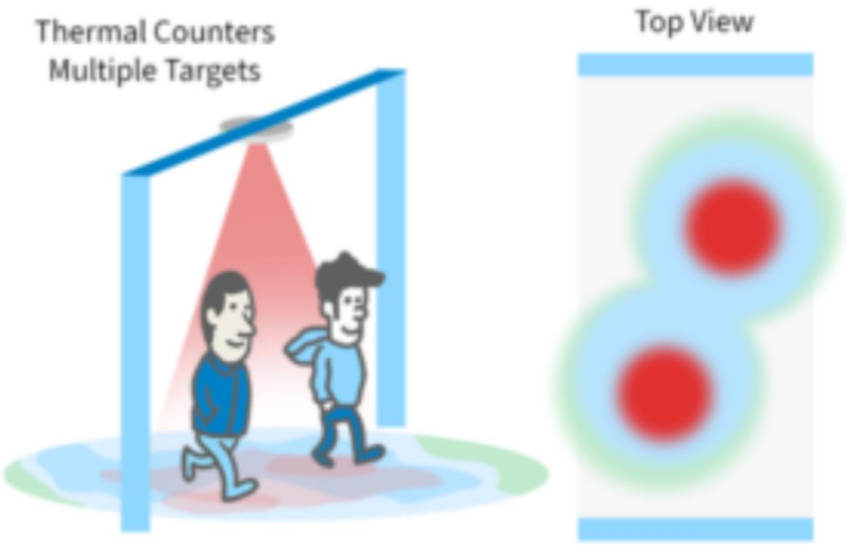


Obrázek 8 - Paprskový senzor

Tepelné senzory využívají teplotu těla zákazníků ke sledování vstupů či pohybu v místnosti. Přesnost tohoto řešení počítání lidí je velmi vysoká, zejména v oblastech s velkým množstvím okolního světla. Funguje také dobře v oblastech se slabým osvětlením, což je výhodné pro bezpečnost. Podobně jako u paprskových senzorů mohou být tepelné systémy počítání osob bezdrátové, ale na rozdíl od výše uvedeného systému lze rozsahy teplotních senzorů rozšířit tak, aby vyhovovaly téměř jakémukoli uspořádání nebo velikosti budovy pomocí opakovačů [26].

Výhodou jsou přesná data o více směrném pohybu zákazníků uvnitř i vně sledované oblasti. Široké vchody jsou pokryty s vysokou mírou přesnosti. Ve skutečnosti je přesnost technologie tepelných senzorů 95 % i vyšší [26].

Nevýhodu jsou dražší náklady kvůli vylepšené technologii. Nižší rozlišení a zorné pole ztěžují rozlišení mezi dospělými a dětmi, což může ovlivnit demografickou přesnost. Zákazníci také musí být v pohybu, aby senzor zachytil jejich signál. Přesnost snímače mohou také bránit vnější povětrnostní podmínky [26].

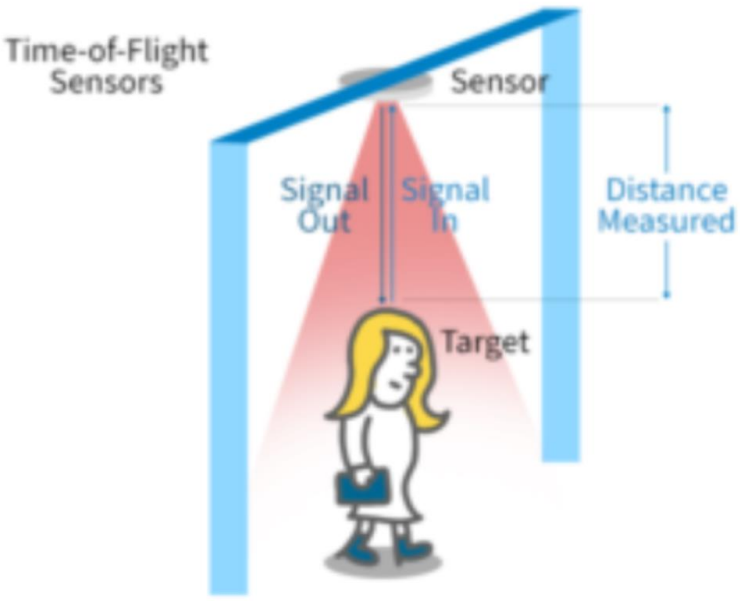


Obrázek 9 - Tepelný senzor

Senzory typu Time-of-Flight (ToF, volně přeloženo jako senzory doby letu) fungují na principu měření vzdálenosti od okolních předmětů v záběru. Tato metoda počítá časový rozdíl mezi vypuštěním signálu ze senzoru a jeho návratem do senzoru. Pro měření se využívá světelných paprsků a ultrazvuku.

Nevýhodou je, že sluneční světlo vyzařuje celé barevné spektrum a může výrazně narušit zpracovávaný signál. Je známo, že senzory typu ToF poskytují nesprávné informace kvůli kvalitě signálu, která se snižuje s rostoucí vzdáleností mezi objektem a senzorem. Rozlišení této senzorové technologie je nízké, takže poskytuje nízkou úroveň přesnosti, pokud jde o počítání objektů. V přeplněných vchodech může být výkon ve srovnání s jinými technologiemi slabý, protože senzory ToF nemusí účinně rozlišovat objekty od návštěvníků nebo dospělých od dětí atd [25].

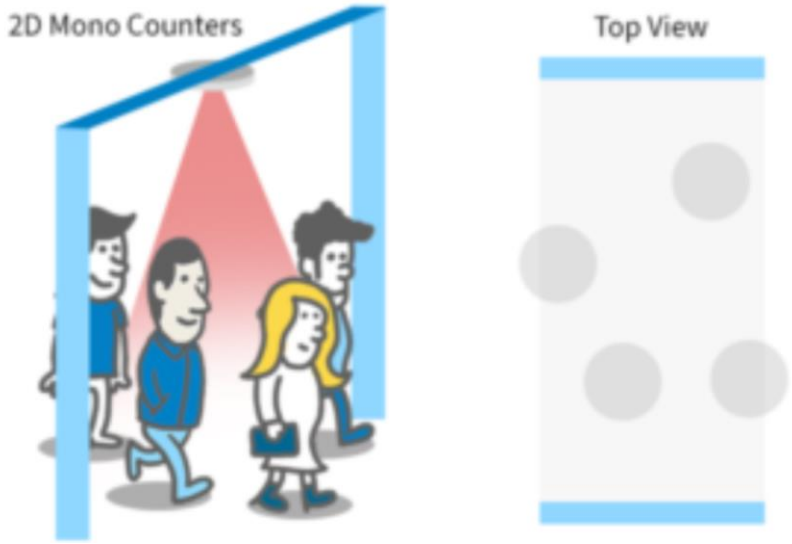
Výhodou naopak je, že senzory doby letu mohou pracovat v naprosté tmě, ale vyžadují více senzorů k pokrytí širší oblasti, což zvyšuje celkové náklady [25].



Obrázek 10 - Time-of-Flight senzor

2D Mono senzory používají k počítání jednu čočku fotoaparátu. Senzory jsou instalovány shora dolů, aby detekovaly pouze pohybující se objekty. Algoritmus počítání lidí digitálně odstraňuje statické pozadí a sleduje pouze pohybující se objekty [25].

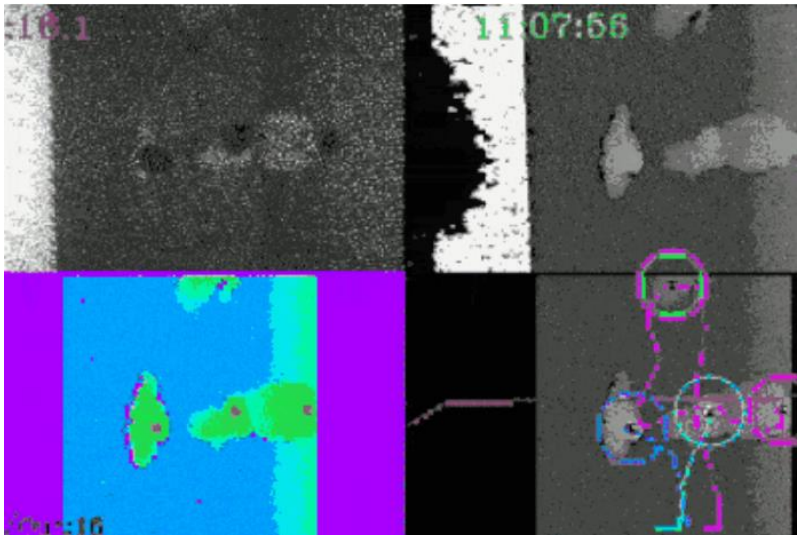
Protože mono senzory postrádají hloubku vidění, neexistuje žádný inteligentní algoritmus detekce objektů, tudíž každý pohybující se objekt se počítá. Díky těmto vlastnostem jsou náchylné k chybnému počítání ve stinném prostředí, a proto se používají v oblastech s nízkým provozem, kde je osvětlení jasné a konzistentní. Jelikož. Zároveň jsou však cenově výhodné a snadno se instalují, ale poskytují nepřesná data, která jsou závislá na prostředí [25].



Obrázek 11 - 2D Mono senzor

3D stereo senzor poskytuje aktivní stereo vidění, napodobuje lidské vidění. Jeho vylepšený modul se však promítá do monitorované oblasti a generuje informace o hloubce i za velmi špatných či žádných světelných podmínek. Technologie 3D aktivního stereo vidění zpracovává kombinované obrazy a vytváří hloubkové mapy, které poskytují přesné a spolehlivé počítání. Senzory jsou instalovány na stropě pro sledování vstupu ze shora [25].

Na Obrázek 12 můžeme vidět vzorový vstup s trojrozměrnými informacemi o hloubce bez světelných podmínek. Hlavy návštěvníků jsou označeny červeným kroužkem. Algoritmus sleduje tento kruh. Vzhledem k tomu, že objekty jsou rozlišeny svou výškou, lze objekty umístěné vedle sebe správně počítat. Tato technologie má vysoké zorné pole, aby pokryla celou plochu, čímž se snižují celkové náklady zákazníka [25].



Obrázek 12 - 3D stereo senzor

3.7.2. Senzor množství CO_2

Jedním z dalších způsobů, jak lze monitorovat obsazenost budov je sledování hladiny oxidu uhličitého (CO_2). Ačkoli jsme schopni jednoznačně porovnávat změnu koncentrace CO_2 v poměru k přítomnosti osob v místnosti, odhadovat přesný počet je velmi náročné. Ovlivňující faktory jsou například tělesná aktivita nebo kondice. Vyšší aktivita nebo srdeční tep osoby v místnosti se projevuje na produkci CO_2. Proto je tato metoda velmi nepřesná, ale pro lepší výsledky je vhodné doplnit monitorovací ekosystém o další senzory jiných typů [15].

3.7.3. Senzor teploty

Pomocí tepelných senzorů lze na stejném principu jako za pomocí senzoru CO_2 sledovat hladinu teploty v objetu. Každé lidské tělo vydává jistou hodnotu tepla do prostoru v kolem sebe. V uzavřených místnostech tedy lze počítat průměrný nárůst teploty a tím se pokusit odhadnout přibližný počet osob nacházejících se na sledovaném místě. To vše je relativně možné jen u velmi dobře hlídaného prostředí. V realitě do těchto údajů vstupují velmi prudce okolní podmínky, jako například otevřená okna či dveře, zesílené topení, zapnutá klimatizace nebo rozsvícená světla vydávající teplo. Z těchto důvodů je monitoring

obsazenosti budov založený pouze na teplotních senzorech velmi složitý. Může však hrát roli v dalších měřeních společně s ostatními daty z jiných senzorů.

3.7.4. Senzor detekce pohybu

Senzor detekce pohybu je elektronické zařízení, které slouží k detekci fyzického pohybu v daném prostoru a převádí pohyb na elektrický signál. Detekce pohybu hraje důležitou roli v zabezpečení objektů či místností. Tyto senzory se využívají na místech, kde by neměl být detekován žádný pohyb a je tedy snadné si všimnout přítomnosti někoho, kdo by se ve sledovaném místě neměl nacházet [27].

Senzory se především používají pro systémy detekce narušení objektů, automatické ovládání dveří atd. Mohou však sloužit i jinak. Senzory pohybu mohou také dešifrovat různé typy pohybů, díky čemuž jsou užitečné v některých odvětvích, kde je nutné pohyby umět rozeznat. Příkladem mohou být i gesta, kdy osoba může zamávat na senzor a tím automaticky požádat třeba o pomoc [27].

3.8. Programovací jazyky

Programovací jazyky jsou formální jazyky určené ke sdělování instrukcí počítači. Tyto jazyky umožňují programátorům psát zdrojový kód způsobem, který může být překladačem nebo interpretem přeložen do strojového kódu, který je pak počítačem prováděn. Programovací jazyky poskytují soubor pravidel a syntaxí pro vytváření programů, které mohou provádět různé úlohy, a to od jednoduchých výpočtů až po složité algoritmy umělé inteligence. Lze je použít k vývoji aplikací, tvorbě webových stránek, automatizaci úloh a mnoha dalším činnostem.

3.8.1. Značkovací jazyk HTML

HTML je zkratka pro HyperText Markup Language. Je to značkovací jazyk používaný k vytváření a strukturování obsahu na webu. Jazyk HTML umožňuje vývojářům webových stránek definovat a formátovat text, obrázky, videa či další média. Umožňuje také vytvářet hypertextové odkazy, které uživatelům dovolují přecházet mezi webovými stránkami [28].

Jazyk HTML používá k definování struktury a obsahu webových stránek sadu značek a atributů. Značky se používají k definování různých typů obsahu, jako jsou nadpisy, odstavce, seznamy, obrázky a odkazy. Atributy poskytují další informace o značce, například zdroj obrázku nebo cíl odkazu. Jazyk HTML je základem webu a používá se spolu s dalšími technologiemi, jako jsou CSS a JavaScript, k vytváření vizuálně atraktivních a interaktivních webových stránek [28].

3.8.2. Kaskádové styly CSS

CSS (Cascading Style Sheets) je jazyk stylů používaný k definici rozvržení, formátování a vizuálního vzhledu dokumentů HTML. Používá se k oddělení prezentace dokumentu od jeho obsahu, což umožňuje větší flexibilitu a kontrolu nad zobrazením webových stránek [29].

Pomocí CSS mohou návrháři a vývojáři definovat styly pro jednotlivé prvky nebo skupiny prvků na webové stránce, například velikost písma, barvu, výplň, okraje, obrázky na pozadí a další. Tyto styly lze aplikovat na konkrétní značky HTML nebo na celé třídy značek, což usnadňuje vytváření konzistentních a jednotných návrhů napříč webovými stránkami [29].

CSS funguje na kaskádovém principu, což znamená, že na jeden prvek lze použít více stylů a prohlížeč určí, který styl má přednost, na základě specifičnosti selektoru a pořadí, v jakém jsou styly definovány. To umožňuje vysokou míru kontroly nad vzhledem webové stránky a zároveň umožňuje snadné aktualizace a změny stylů webových stránek [29].

3.8.3. Skriptovací jazyk PHP

PHP (Hypertext Preprocessor) je skriptovací jazyk na straně serveru používaný především pro vývoj webových stránek. Původně jej v roce 1994 vytvořil Rasmus Lerdorf jako sadu skriptů CGI pro sledování návštěvníků svých webových stránek. Postupem času se PHP vyvinul ve výkonný programovací jazyk používaný k vytváření dynamických webových aplikací.

Kód PHP se spouští na serveru a generuje jazyk HTML, který se odesílá do webového prohlížeče klienta. To umožňuje vytvářet dynamické webové stránky, které se mohou měnit na základě vstupu uživatele, obsahu databáze a dalších faktorů.

Jazyk PHP se často používá ve spojení s databázemi, jako je MySQL, k vytváření webových aplikací, které umožňují uživatelům pracovat s daty v reálném čase. Jedná se o otevřený zdrojový kód, což znamená, že je možné jej používat a upravovat zcela zdarma.

3.8.4. Arduino IDE

Arduino je integrované vývojové prostředí neboli Arduino Software (IDE). Obsahuje textový editor pro psaní kódu, oblast zpráv, textovou konzoli, panel nástrojů s tlačítky pro běžné funkce a řadu nabídek. Připojuje se k hardwaru Arduino a umožňuje nahrávat programy a komunikovat se zařízeními [30].

Programy napsané pomocí softwaru Arduino se nazývají náčrty. Tyto náčrty se píší v textovém editoru a ukládají se s příponou *.ino*. Editor má funkce pro vyjmutí/vložení a pro vyhledávání/nahrazování textu. Oblast zpráv poskytuje zpětnou vazbu při ukládání a exportu a také zobrazuje případné chyby. Konzole zobrazuje textový výstup softwaru Arduino, včetně kompletních chybových hlášení a dalších informací. V pravém dolním rohu okna se zobrazuje nakonfigurovaná deska a sériový port. Tlačítka na panelu nástrojů umožňují ověřovat a nahrávat programy, vytvářet, otevírat a ukládat náčrty a otevírat sériový monitor [30].

3.9. IEEE 802.11

Standart IEEE 802.11 označuje soubor norem, které definují komunikaci pro bezdrátové sítě (Wireless Local-Area Network, WLAN). Jak již název napovídá, na normu IEEE 802.11 dohlíží organizace IEEE. Technologie 802.11 je obecně označována jako WiFi.

Bezdrátová lokální síť WLAN je skupina počítačů nebo jiných zařízení, která tvoří síť založenou na rádiovém přenosu, nikoli na kabelovém připojení. Síť WiFi je typem sítě WLAN. Každý, kdo je připojen k síti WiFi a čte libovolnou webovou stránku, používá právě síť WLAN. Stejně jako vysílací média přenáší WLAN informace prostřednictvím rádiových vln. Data se posílají v paketech. Pakety obsahují vrstvy se štítky a instrukcemi, které spolu s jedinečnými MAC adresami přiřazenými koncovým bodům umožňují směrování na určená místa [31]. Síť WLAN lze konfigurovat dvěma způsoby: podle infrastruktury a ad-hoc.

Konfigurace dle infrastruktury – příkladem sítě WLAN nastavené v režimu infrastruktury je domácí nebo kancelářská síť WiFi. Všechny koncové body jsou propojeny a komunikují spolu prostřednictvím základnové stanice, která může také poskytovat přístup k internetu. Základní infrastrukturní síť WLAN lze nastavit pouze ze dvou částí [31]:

- z bezdrátového směrovače, který funguje jako základnová stanice. Ve většině případů je bezdrátový směrovač zároveň internetovým připojením,
- z koncových bodů, kterými mohou být počítače, mobilní zařízení, tiskárny a další zařízení.

Ad-hoc konfigurace – v tomto uspořádání síť WLAN propojuje koncové body, jako jsou počítačové pracovní stanice a mobilní zařízení bez použití základnové stanice. Použití technologie WiFi Direct je pro bezdrátovou síť ad-hoc běžné. Síť WLAN ad-hoc se snadno nastavuje a může poskytovat základní komunikaci peer-to-peer. Ad-hoc síť WLAN vyžaduje pouze dva nebo více koncových bodů s vestavěným rádiovým přenosem, jako jsou počítače nebo mobilní zařízení [31].

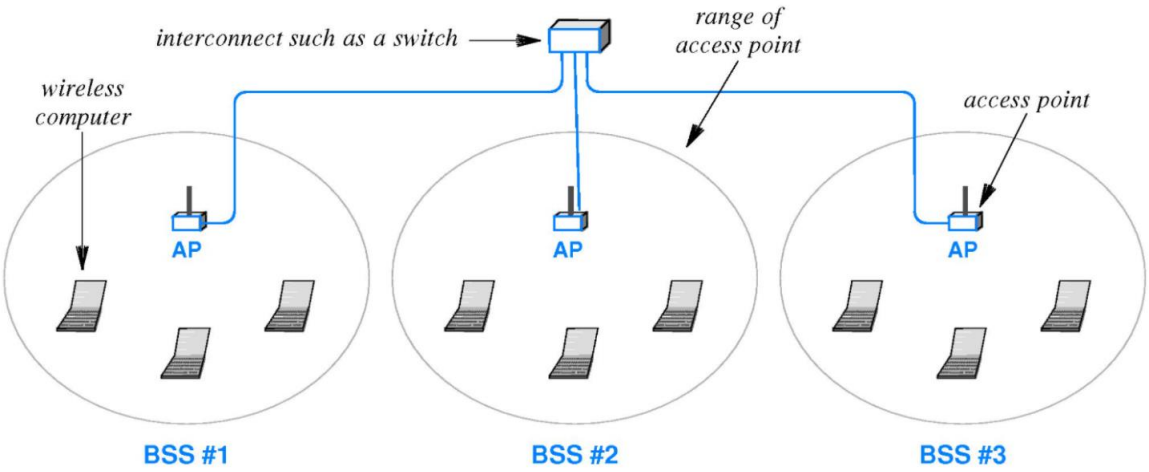
3.9.1. Architektura WLAN

Architektura WLAN se odvíjí od normy IEEE 802.11. Skládá se z několika základních komponent:

- stanice,
- základní sada služeb (BSS),
- distribuční systém,
- přístupový bod (AP),
- most,
- koncový bod.

Stanice jsou síťové komponenty, které komunikují bezdrátově. Mohou to být přístupové body nebo koncové body a každá z nich má svou vlastní síťovou adresu. BSS (Basic Service Set) je síť, která spojuje skupinu stanic. Nezávislá BSS je soubor stanic v sítích ad-hoc. Rozšířená sada služeb je soubor propojených BSS, které se vyskytují například v síti s mnoha přístupovými body. Distribuční systém spojuje přístupové body. K dispozici jsou kabelová nebo bezdrátová připojení. Pevný bezdrátový přenos je typ rádiového přenosu, který se používá k propojení dvou geograficky oddělených přístupových bodů [32].

Přístupový bod je základnová stanice, která slouží jako přípojný bod pro ostatní stanice. Termín „přístup“ se vztahuje k síťovému připojení stanic, ale může se vztahovat i na přístup k internetu, protože mnoho směrovačů fungují také jako modemy. K propojení přístupových bodů lze použít ethernetové kabely nebo bezdrátová připojení. Most sítě WLAN spojuje síť WLAN se sítí LAN nebo přístupovým bodem. Koncový bod je počítač, mobilní zařízení, tiskárna nebo IoT zařízení používané uživatelem [32].



Obrázek 13 - Schéma architektury WLAN

3.9.2. Zabezpečení WLAN

Sítě WLAN jsou náchylnější ke kybernetickým útokům než fyzické sítě. Hacker v kabelové síti musí fyzicky získat přístup do vnitřní sítě nebo prolomit vnější firewall. U sítě WLAN stačí, aby se hacker dostal do jejího dosahu [32].

Jedním z nejzákladnějších přístupů k zabezpečení sítě WLAN je blokování nežádoucích stanic pomocí MAC adres. Nicméně je i tak možné se připojit k síti zfalšováním schválené adresy. Nejrozšířenějším přístupem k zabezpečení sítě WLAN je šifrování, například WEP a WPA, přičemž obvyklou metodou ověřování je WPA2 [32].

3.10. Databázový systém MySQL

MySQL je nejpopulárnější open source systém pro správu databází SQL, kterou vyvíjí, distribuuje a podporuje společnost Oracle Corporation. Databáze je strukturovaný soubor dat. Může se jednat o cokoli od jednoduchého nákupního seznamu až po obrovské množství informací v podnikové síti. K přidávání, přístupu a zpracování dat uložených v počítačové databázi potřebujete systém pro správu databáze, například MySQL Server [33].

Vzhledem k tomu, že počítače velmi dobře zvládají zpracovávat velké objemy dat, hrají systémy správy databází ústřední roli ve výpočetní technice, ať už jako samostatné nástroje nebo jako součásti jiných aplikací [33].

Relační databáze ukládají data do samostatných tabulek, místo aby všechna data ukládala do jednoho velkého skladu. Struktury databáze jsou uspořádány do fyzických souborů optimalizovaných pro rychlost. Logický model s objekty, jako jsou databáze, tabulky, pohledy, řádky a sloupce, nabízí flexibilní programovací prostředí. Lze nastavovat pravidla upravující vztahy mezi různými datovými poli, jako jsou vztahy 1:1 nebo 1:N. Databáze tato pravidla vynucuje, takže díky dobře navržené databázi se vaše aplikace nikdy nesetká s nekonzistentními, duplicitními, osiřelými nebo neaktuálními či chybějícími daty [33].

MySQL Server může pohodlně běžet na stolním počítači nebo notebooku vedle dalších aplikací, webových serverů apod. a nevyžaduje žádnou nebo jen minimální pozornost. Server MySQL byl původně vyvinut pro zpracování velkých databází mnohem rychleji než stávající řešení a již několik let se úspěšně používá ve vysoce náročných produkčních prostředích. Přestože je MySQL Server neustále vyvíjen, nabízí dnes bohatou a užitečnou sadu funkcí. Díky své konektivitě, rychlosti a zabezpečení je MySQL Server velmi vhodný pro přístup k databázím na internetu [33].

4. Vlastní práce

V této sekci se budeme podrobněji věnovat analýze jednotlivých stávajících řešení. Analýza je zaměřena konkrétně na dvě stávající řešení. Prvním je projekt WOLNO, který je aktivně využívaný v prostorech Provozně ekonomické fakulty na České zemědělské univerzitě v Praze. Druhým a zároveň primárním řešením, kterým se bude analýza zabývat je prototyp od Ing. Jana Poláčka z loňského roku (2022), který tvořil v rámci své diplomové práce. Z dostupných a analyzovaných dat se pokusíme vyvodit komplexní zhodnocení obou řešení a navrhnou nový prototyp rozšířený o další funkce, které by mohli být užitečné pro monitorování obsazenosti budov. Následně rozebereme postup tvorby prototypu, jeho výhody, nevýhody nebo komplikace, které během projektu nastaly. Postup práce je tematicky rozdělen do 5 základních částí:

- analýza stávajícího řešení,
- návrh hardware prototypu,
- softwarové řešení,
- vizualizace dat,
- testování.

4.1. Analýza stávajícího řešení

Začátkem praktické části této diplomové práce je zjištění současného stavu již aktivních řešení. Tudíž je nutné provést alespoň částečně analýzu stávajícího stavu řešení, což je proces, který má za úkol zhodnotit aktuální stav projektu, problému nebo situace a určit, co funguje dobře a co by mohlo být zlepšeno. Postup analýzy stávajícího stavu řešení se obecně skládá z následujících kroků:

- shromáždění informací,
- identifikace klíčových faktorů,
- zhodnocení rizik,
- vyvození závěrů.

Stávajícím řešením je myšlena diplomová práce Ing. Jana Poláčka na téma „Využití internetu věcí pro monitoring obsazenosti budov“. Současně však existuje již zmíněný monitorovací systém WOLNO (dále jen původní řešení), který je aktivně využívaný v budově Provozně ekonomické fakulty České zemědělské univerzity v Praze. Tento systém je zde okrajově zmíněný, jelikož pan inženýr Poláček z něj vycházel jako stávající řešení pro svou diplomovou práci. Cílem této diplomové práce však zůstává analýza jeho diplomová práce.

4.1.1. Monitorovací systém WOLNO

Aplikace WOLNO poskytuje informace o obsazenosti oblastí v areálu na základě provozních parametrů bezdrátové infrastruktury univerzitní WiFi sítě. Studenti se díky tomu mohou podívat, kde je aktuálně nejvíce lidí a podle toho si např. vybrat místo, kde budou mít nejvíce klidu pro studium [21].

Obrázek 14 - Logo systému WOLNO

Pilotní projekt je realizován v rámci Provozně ekonomické fakulty, kde pokrytí Wifi signálem zajišťuje řada jednotlivých AP (přístupových bodů). Na základě jejich rozložení v prostoru byly vydefinovány jednotlivé sektory, které jsou v rámci mapy v aplikaci WOLNO obarvovány barevnou škálou znázorňující index obsazenosti. Index obsazenosti vychází z počtu připojených uživatelů k jednotlivým WiFi sítím (AP). Aplikace poskytuje elementární nástroje pro základní uživatelskou analýzu historických dat. Je tak možné například filtrovat určitý časový interval, pro který se zobrazí data. Aplikace také poskytuje graf průměrné obsazenosti v čase. Může tak sloužit pro optimalizaci využití odpočinkových a studijních prostor [21].

Při analýze tohoto řešení však byly zjištěny následující nedostatky. Hlavním nedostatkem je, že systém pracuje pouze s uživateli připojenými ke školní bezdrátové WiFi síti. Připojit k této síti se mohou jen uživatelé roamingové infrastruktury Eduroam, což bývají zpravidla studenti a zaměstnanci univerzit. Lze předpokládat, že se v prostorech vyskytují i osoby, které síť využívat nemohou, jelikož nemají potřebné oprávnění k využívání sítě nebo jen nejsou připojeni k síti WiFi [15].

4.1.2. Využití internetu věcí pro monitoring obsazenosti budov

Stávající řešení vychází ze systému WOLNO a je založen na asociačním procesu a řídících rámcích standartu IEEE 802.11. Toto řešení je navrženo tak, aby bylo schopné monitorovat téměř veškerá zařízení v blízkém okolí pomocí WiFi. Aby monitorování bylo úspěšné, je potřeba aby zařízení mělo zapnutý WiFi adaptér. V opačném případě k detekci nedoje což se jeví jako nevýhoda stávajícího řešení.

K dosažení počtu zařízení je zde použita metoda detekce sondovacích rámců Probe Request. Jedná se o metodu aktivního naslouchání, při které se v pravidelných intervalech vysílají rámce Probe Request s dotazem, jaká síť je na daném kanálu dostupná. Tímto způsobem je následně možné identifikovat okolní zařízení s aktivním WiFi adaptérem. V tomto řešení jsou primárními sledovanými údaji MAC adresy a RSSI. MAC adresa je unikátním identifikátorem zařízení v síti. RSSI je indikátorem intenzity signálu. Právě díky MAC adresám je možné ve stávajícím řešení počítat okolní zařízení. Jelikož se jedná o unikátní označení, je možné následně kvantifikovat. Na základě zjištěného počtu zařízení je následně snaha o odhad počtu osob pomocí metody proximity. Odhad je určován pomocí přijímače, který dekóduje paket vyslaný vysílačem. V těchto lokalizačních systémech je poloha určena na základě polohy nejbližšího vysílače. Přesnost lokalizace pak závisí na hustotě sítě vysílačů.

Jak již bylo řečeno výše, hlavní nevýhodou stávajícího řešení je skutečnost, že musí mít zařízení vždy aktivní WiFi adaptér, aby mohly být detekovány. Což nemusí mít ve výsledku vždy vypovídající hodnoty. Jelikož v dnešní době jsou neomezená data poskytovaná mobilními operátory stále běžnější a dostupnější, nutnost používat WiFi na

svém chytrém zařízení je tedy stále menší. Sekundárním problémem je i fakt, že pomocí tohoto řešení je možné docílit pouze přesného počtu zařízení (sčítáním MAC adres) a následně odhadovat počet osob. To nemusí být vždy vhodné či žádoucí.

Návrhem na zefektivnění sbíraných monitorovacích dat je rozšíření stávajícího řešení o novou metodu pozorování. Stávající řešení bude obohaceno o paprskovou virtuální závoru, která může být umístěna v primárních vstupech či průchodech monitorované oblasti. Dosáhneme tedy přesnějšího měření a zároveň bude možné spočítat přesný počet zařízení i osob ve sledované oblasti. Tyto informace mohou být dále aplikovány například ke zjištění průměrného počtu nositelných WiFi zařízení na jednu osobu. To může být zajímavý indikátor v rámci nějaké dlouhodobější analýzy vývoje informačních technologií.

4.2. Návrh hardware prototypu

Aby bylo možné navrhnout HW prototyp, bylo nutné nastudovat informace v teoretické části diplomové práce a z poznatků stávajícího a původního řešení bylo následně možné navrhnout první schéma nového HW prototypu a jeho základní funkce. Prototyp má dvě stěžejní funkcionality. Dokáže zpracovávat dva druhy informací. Každý druh informace zpracovává jiná řídící jednotka. Prototyp je tedy složen ze dvou řídících jednotek.

Prvním funkcí je WiFi sniffer (také známý jako WiFi scanner), což je nástroj, který umožňuje monitorovat a analyzovat bezdrátové sítě WiFi. Jedná se o software, který lze nainstalovat na zařízení s WiFi adaptérem, jako je například notebook, smartphone, tablet nebo v tomto případě na řídící jednotku Wemos D1 Mini. WiFi sniffer umožňuje uživatelům procházet dostupné WiFi sítě v okolí a získávat informace o síti, jako je například název sítě, síla signálu, kanál, typ šifrování a další. Tyto informace mohou být užitečné pro správce sítí, kteří potřebují vědět, jaké sítě jsou v okolí a jak silný je jejich signál. Pro účely této diplomové práce je WiFi sniffer použit k počítání zařízení (mobilních telefonů, chytrých hodinek, notebooků, tabletů apod.) připojených k WiFi. Tato metoda je velmi účinná a rozšířená, avšak z nasbíraných hodnot lze vyčíst pouze hustotu WiFi zařízení v určité monitorované místnosti nebo sektoru, nikoli přesný počet osob. Z tohoto důvodu je prototyp obohacený o další funkci.

Druhou funkcí prototypu jsou dva paprskové senzory. Tento senzor slouží jako další zdroj informací. Tyto dva zdroje lze následně mezi sebou porovnat a dosáhnout tak mnohem přesnějších výsledků. V prototypu jsou použity dva senzory (vstupní a výstupní). Je to proto, že paprskové senzory nejsou schopny rozeznat směr pohybu osoby/objektu skrze sledovanou virtuální závoru. Je tedy nutné mít senzory dva a vždy sledovat, který zaznamená pohyb jako první. Následně pak osobu z místnosti přičte nebo odečte.

4.2.1. Řídící deska Wemos D1 Mini

Jako řídicí jednotky prototypu byly zvoleny dvě desky Wemos D1 mini. Tato řídící deska je populární vývojová deska založená na mikrokontroleru ESP8266. Má malé rozměry, podobné jako Arduino Pro Mini a je určena pro projekty založené na WiFi. Mezi její hlavní specifikace patří:

- mikrokontroler ESP8266 (80 MHz, 4 MB paměti flash),
- integrovaný modul WiFi (802.11 b/g/n),
- 11 digitálních vstupních/výstupních pinů (včetně 1 PWM výstupu),
- 1 analogový vstup (max. vstupní napětí 3,2 V),
- micro USB port pro napájení a programování,
- kompatibilní s Arduino IDE.

Obrázek 15 - Wemos D1 Mini (clone)

Wemos D1 Mini se často používá pro projekty internetu věcí, jako je domácí automatizace, záznam dat nebo vzdálené monitorování. Lze jej programovat například pomocí prostředí Arduino IDE. Kromě toho je pro řídící desku Wemos D1 Mini k dispozici mnoho štítů a modulů, včetně senzorů, relé a displejů, které lze k desce snadno připojit pomocí pinových hlaviček.

4.2.2. Paprskové senzory

V rámci HW prototypu byly použity dva typy paprskových senzorů. Jedná se o virtuální závoru, která je schopna zaznamenat průchody osob touto závorou. Jsou zde použity dva typy senzorů. Primárním důvodem je fakt, že paprskové senzory nejsou schopny rozpoznat směr pohybu skrz závoru. Tudíž je nutné instalovat jednu závoru zvenku průchodu a druhou zevnitř. Tímto způsobem je následně možné rozeznat směr průchodu a na základě toho rozhodnout, zda se jedná o příchod nebo odchod z místnosti. Princip počítání průchodů je prostý. V případě, že zaznamená pohyb senzor A dříve než senzor B, jedná se o příchod. V opačném případě se jedná o odchod. Sekundárním důvodem použití dvou rozdílných senzorů bylo otestování funkčnosti mezi nimi.

Prvním typ paprskového senzoru je dražší a složitější, který je schopen blikat. To může být výhodou, jelikož díky blikání se senzor stává odolnějším vůči okolním vlivům. Naopak má tento senzor poměrně vysoké napájení 12 V a je zbytečně drahý.

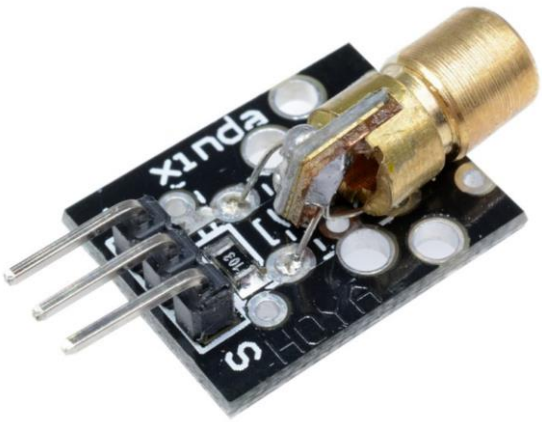
Obrázek 16 - Paprsková závora (stavebnice)

Tento senzor byl pořízen jako sada (stavebnice) od společnosti FLAJZAR, která tyto typy senzorů vyrábí. Specifikace paprskové závory jsou následující:

- napájení 12 V
- max. odběr proudu (laser svítí, relé drží): 65 mA
- typ laseru: polovodičový laser, výkon max. 5 mW, třída 3 A, vlnová délka 30-680 nm
- pracovní dosah závory: teoreticky až několik stovek metrů, prakticky lze použít na cca 50-100 metrů (bez optiky)
- rozměry plošných spojů: 42 x 37 mm
- rozměry plastových krabiček: 47 x 42 x 22 mm (bez úchytů)
- zatížení kontaktu relé: 100 mA (odporová zátěž)
- pracovní teplota: vnitřní provedení 0 až 40 °C, venkovní provedení -15 °C až 40 °C.

Druhý typ použitého paprskového senzoru je výrazně levnější, jednodušší a má nižší napájení 5 V. Nevýhodou je absence blikání, díky kterému je závora odolnější vůči okolnímu rušení. Funkcionalita by však mohla být dodělána připojením na jeden z volných pinů na řídící desce Wemos. Laser i deska Wemos mají napájení 5 V, nebyl by tedy téměř žádný problém funkci přidat. Tento senzor nebyl pořízen jako kompletní sada. Byl sestrojen pomocí dvou samostatných dílů.

Jedním dílem je laserový modul 650 nm 5 mW 5 V, který vydává červený paprsek. Je tedy vysílačem již zmíněné závory.



Obrázek 17 - Laserový modul

Druhým dílem je digitální světelný senzor s regulací. Obsahuje fotorezistor a potenciometr. Tento senzor je přijímačem paprsku z laserového modulu. V případě, kdy dojde k přerušení vysílaného paprsku do přijímače, senzor zaznamená průchod.

Obrázek 18 - Digitální světelný senzor

4.2.3. Baterie 9 V (napájení)

O napájení celého prototypu se stará napájecí baterie 9 V, což je malá a kompaktní baterie, která se používá k napájení různých elektronických zařízení, jako jsou různé detektory, bezdrátové mikrofony, hudební nástroje a mnoho dalších. Tento typ baterie má typické rozměry 48,5 x 26,5 x 17,5 mm a obvykle obsahuje šest oddělených galvanických článků, které jsou uspořádány tak, aby poskytovaly výstupní napětí 9 voltů. Baterie může být vyrobena z různých chemických složek, jako jsou alkalické nebo lithiové baterie, což ovlivňuje výkon a délku životnosti baterie.

Obrázek 19 - Napájecí baterie 9 V

4.3. Softwarové řešení

V rámci diplomové práce byly zpracovány celkem 4 rozdílné softwarové řešení. Jedná se o navržený software pro WiFi sniffer, virtuální paprskovou závoru, pro webovou aplikaci a použité databázové prostředí. Každé s těchto řešení je nedílnou součástí navrženého prototypu. Zároveň je nutné zmínit, že pouze dva z uvedených softwarů byly navrženy v prostředí Arduino IDE a následně nahrány do HW prototypu, konkrétně do dvou řídících desek (jedna řídící deska má pouze jeden nahraný software).

Software pro webovou aplikaci stojí samostatně mimo prototyp. Webová aplikace byla napsána jako vizualizační prostředí, kde lze zobrazit sebraná data pomocí prototypu. Aplikace je souhrn značkovacího jazyku HTML, formátovacích stylů CSS a programovacího jazyka PHP. Součástí je i knihovna Bootstrap, což je otevřená sada nástrojů kaskádových stylů pro tvorbu webu a webových aplikací.

Databázové prostředí zde slouží jako datový sklad pro nasbíraná data. Databáze obsahuje dvě relační tabulky, do kterých se data ukládají. Jedna relační tabulka obsahuje hodnoty nasbírané z virtuální paprskové závory a druhá z WiFi snifferu. Výsledná data a grafy jsou následně vypisována v rámci webové aplikace.

4.3.1. Webová aplikace

Pozadí webová aplikace je tvořena celkem pěti soubory PHP a jedním souborem CSS. Primárním souborem soubor *index.php*, který zobrazuje výslednou webovou aplikaci. Tento soubor obsahuje převážně prvky HTML, které definují strukturu aplikace. Do tohoto souboru je zároveň linkován *function.php*. Jedná se soubor obsahující 5 základních funkcí, které webová aplikace nabízí. Seznam funkcí je následující:

- createDbConnection,
- getPassageTable,
- getPassageGraphData,
- getUniqMacTable,
- getUniqMacGraphData.

Funkce *createDbConnection* slouží k propojení webové aplikace s databázovým prostředím. Pomocí ní lze definovat přístupové údaje (hosting, uživatelské jméno, heslo a název databáze) do databáze. Po navázání spojení je následně možně data vkládat, vypisovat, mazat apod.

```php
function createDbConnection(){
    //DB CONNECTION
    $config = array(
        "hostname" => "your_hostname",
        "dbuser" => "your_dbuser",
        "dbpassword" => "your_dbpassword",
        "dbname" => "your_dbname"
    );

    $mysqli = mysqli_connect($config['hostname'], $config['dbuser'], $config['dbpassword'], $config['dbname']);

    //CHECK CONNECTION
    if (mysqli_connect_errno()){
        $err = "Connect failed:" . mysqli_connect_error();
        echo $err;
    }

    return $mysqli;
}
```

Obrázek 20 - Funkce createDbConnection

Funkce *getPassageTable* nabízí přehledný výpis dat o počtech průchodů z databáze. Data se vypisují do PHP generované tabulky. Výpis obsahuje informace o ID záznamu, datumu zápisu, absolutní hodnotu 1 a typ průchodu. Pro zisk dat z databáze je použit následující SQL příkaz:

> SELECT * FROM passage WHERE `date` >= date(\"".$date."\") AND `date` < date(\"".$date."\") + INTERVAL 1 DAY ORDER BY `date`;

```php
function getPassageTable($date){
    $mysqli = createDbConnection();

    //SELECT ALL DATA FROM PASSAGE DB
    $sql = "SELECT * FROM passage WHERE `date` >= date(\"".$date."\") AND `date` < date(\"".$date."\") + INTERVAL 1 DAY ORDER BY `date`;";
    $result = $mysqli->query($sql);

    $record = 1;

    while ($obj = $result->fetch_object()){
        $tableBody = $tableBody .
        "<tr>
            <td>" . $record++ . "</td>
            <td>" . $obj->date . "</td>
            <td>" . $obj->count . "</td>
            <td>" . $obj->type . "</td>
        </tr>";
    }

    return $tableBody;
}
```

Obrázek 21 - Funkce getPassageTable

Funkce *getPassageGraphData* slouží k přípravě dat pro vizualizaci do grafu. Funkce pracuje s daty příchodů a odchodů, na které se dotazuje databáze a člení hodnoty podle jednotlivých hodin zápisu. Dochází zde k uchování informací do pole *array*, ve kterém proměnná *graphLabels* nabývá hodnot časového rozmezí (po hodinách) a proměnná *graphValues* obsahuje konkrétní počet zaznamenaných osob ve sledovaném prostředí. Pro zisk dat z databáze je použit následující SQL příkaz:

> SELECT HOUR(`date`) AS hours, SUM(`count`) AS `passage`" . "FROM (SELECT * FROM `passage` WHERE DATE(`date`) = DATE('".$date."')) AS T GROUP BY HOUR(`date`)

```php
function getPassageGraphData($date){
    $mysqli = createDbConnection();
    global $checkScriptPassage;

    //SELECT DATA FROM PASSAGE DB AND PREPARE DATA FOR DISPLAY IN GRAPH
    $sql = "SELECT HOUR(`date`) AS hours, SUM(`count`) AS `passage`" . "FROM (SELECT * FROM `passage` WHERE
    DATE(`date`) = DATE('".$date."')) AS T GROUP BY HOUR(`date`)";
    $result_graph = $mysqli->query($sql);

    $sum_count = 0;
    $lastvalue = -1;

    while($row = $result_graph->fetch_object()){
        if ($lastvalue == -1){
            $lastvalue = $row->hours - 1;
        }

        while ($lastvalue < ($row->hours - 1)){
            $graphLabels = $graphLabels . "'" . ($lastvalue + 1) . "',";
            $graphValues = $graphValues . $sum_count . ",";
            $lastvalue = $lastvalue + 1;
        }

        $checkScriptPassage = "passage";
        $sum_count = $sum_count + $row->passage;

        if ($lastvalue == ($row->hours - 1)){
            $graphLabels = $graphLabels . "'" . ($lastvalue + 1) . "',";
            $graphValues = $graphValues . $sum_count . ",";
            $lastvalue = $lastvalue + 1;
        }
    }

    return array('graphLabels' => $graphLabels, 'graphValues' => $graphValues);
}
```

Obrázek 22 - Funkce getPassageGraphData

Funkce *getUniqMacTable* nabízí opět přehledný výpis dat, tentokrát však o počtu unikátních MAC adres zařízení z databáze. Data se vypisují do PHP generované tabulky. Výpis obsahuje informace o datumu zápisu, konkrétní MAC adresu, AP_SSID a počet výskytů dané MAC adresy v databázi. Pro zisk dat z databáze je použit následující SQL příkaz:

> SELECT `date`, `mac`, `ap_ssid`, count(*) AS \"count\" FROM `connectedMac` WHERE `date` >= date(\"".$date."\") AND `date` < date(\"".$date."\") + INTERVAL 1 DAY GROUP BY `mac` ORDER BY `date`;

```
function getUniqMacTable($date){
    $mysqli = createDbConnection();

    //SELECT ALL DATA FROM CONNECTEDMAC DB FOR PRINT TABLE
    $sql = "SELECT `date`, `mac`, `ap_ssid`, count(*) AS \"count\" FROM `connectedMac` WHERE
    `date` >= date(\"".$date."\") AND `date` < date(\"".$date."\") + INTERVAL 1 DAY GROUP BY `mac` ORDER BY `date`;";
    $result = $mysqli->query($sql);

    $record = 1;

    while ($obj = $result->fetch_object()){
        $tableBody = $tableBody .
        "<tr>
            <td>" . $record++ . "</td>
            <td>" . $obj->date . "</td>
            <td>" . $obj->mac . "</td>
            <td>" . $obj->ap_ssid . "</td>
            <td>" . $obj->count . "</td>
        </tr>";
    }

    return $tableBody;
}
```

Obrázek 23 - Funkce getUniqMacTable

Funkce *getUniqMacGraphData* slouží k přípravě dat pro vizualizaci do grafu. Funkce pracuje s daty unikátních MAC adres, na které se dotazuje databáze a člení hodnoty podle jednotlivých hodin zápisu. Dochází zde k uchování informací do pole *array*, ve kterém proměnná *graphLabels* nabývá hodnot časového rozmezí (po hodinách) a proměnná *graphValues* obsahuje konkrétní počet unikátních MAC adres v okolí. Pro zisk dat z databáze je použit následující SQL příkaz:

> SELECT HOUR(`date`) AS hours, COUNT(`mac`) AS `uniqMac`" . "FROM (SELECT * FROM `connectedMac` WHERE DATE(`date`) = DATE('".$date."') GROUP BY `mac`) AS T GROUP BY HOUR(`date`)

```php
function getUniqMacGraphData($date){
    $mysqli = createDbConnection();
    global $checkScriptMac;

    //SELECT DATA FROM CONNECTEDMAC DB AND PREPARE DATA FOR DISPLAY IN GRAPH
    $sql = "SELECT HOUR(`date`) AS hours, COUNT(`mac`) AS `uniqMac`" . "FROM (SELECT * FROM `connectedMac` WHERE
    DATE(`date`) = DATE('".$date."') GROUP BY `mac`) AS T GROUP BY HOUR(`date`)";
    $resultGraph = $mysqli->query($sql);

    $lastValue = -1;

    while ($row = $resultGraph->fetch_object()){
        if ($lastValue == -1){
            $lastValue = $row->hours - 1;
        }

        $checkScriptMac = "mac";

        while ($lastValue <= ($row->hours - 1)){
            $graphLabels = $graphLabels . "'" . ($lastValue + 1) . "',";

            if (($row->hours - $lastValue) == 1){
                $graphValues = $graphValues . $row->uniqMac . ",";
            }else{
                $graphValues = $graphValues . "0" . ",";
            }

            $lastValue = $lastValue + 1;
        }
    }

    return array('graphLabels' => $graphLabels, 'graphValues' => $graphValues);
}
```

Obrázek 24 - Funkce getUniqMacGraphData

Pro vkládání nasbíraných dat z prototypu do databáze bylo vytvořeno API (aplikační softwarové rozhraní), skrze které se data odesílají. Pro tento účel byly vytvořeny dva samostatné soubory *mac.php* a *gate.php*, které obsahují několik ověřujících podmínek pro navázání spojení pro přenos dat, jako například ověření komunikačního tokenu, zda jsou data přijímána skrze metodu POST a jiné. Pokud se všechny tyto definované podmínky splní, dojde k zapsání dat do databáze. V případě zápisu MAC adres dochází ještě k transformaci dat. Získané MAC adresy se nejprve převádí z desetinné číselné soustavy do hexadecimální, hodnotu rozdělní po 2 znacích a následně mezi každou dvojici vloží dvojtečku. Čímž je dosaženou správného formátu MAC adresy pro zápis do databáze. Níže jsou uvedeny dva SQL dotazy, pomocí kterých jsou data zapisována.

> INSERT INTO `connectedMac` (`mac`, `ap_ssid`, `channel`, `ap_mac`, `rssi`, `date`, `room`) VALUES (?, ?, ?, ?, ?, ?, ?)

> INSERT INTO `passage` (`date`, `type`, `count`, `room`) VALUES (?, ?, ?, ?)

```php
//DB CONNECTION
$mysqli = createDbConnection();

//INSERT DATA TO DB
foreach ($decodeds as &$decoded){
    $today = date("Y-m-d G:i:s");

    //TRANSFORM DECIMAL NUMBER TO MAC ADDRESS FORM
    $macHexSplit = str_split(dechex($decoded["mac"]), 2);
    $macAddress = substr(implode(substr_replace($macHexSplit,':',2)),0,-1);

    $apHexSplit = str_split(dechex($decoded["ap_mac"]), 2);
    $apMacAddress = substr(implode(substr_replace($apHexSplit,':',2)),0,-1);

    if ($stmt = $mysqli->prepare("INSERT INTO `connectedMac` (`mac`, `ap_ssid`, `channel`, `ap_mac`, `rssi`, `date`, `room`) VALUES (?, ?, ?, ?, ?, ?, ?)"))
        {
        $stmt->bind_param('ssisiss', $macAddress, $decoded["ap_ssid"], $decoded["chanel"], $apMacAddress, $decoded["rssi"], $today, $decoded["room"]);
        if($stmt->execute()){
            echo "OK";
        }else{
            $err = "Error:" . mysqli_error($mysqli);
            echo $err;
        }
    }else{
        $err = "Error:" . mysqli_error($stmt);
        echo $err;
    }
}
```

Obrázek 25 - Kód pro zápis MAC adres do databáze

```php
//DB CONNECTION
$mysqli = createDbConnection();

//INSERT DATA TO DB
$today = date("Y-m-d G:i:s");

if ($stmt = $mysqli->prepare("INSERT INTO `passage` (`date`, `type`, `count`, `room`) VALUES (?, ?, ?, ?)")){
    $stmt->bind_param('ssis', $today, $decoded["type"], $decoded["count"], $decoded["room"]);
    if($stmt->execute()){
        echo "OK";
    }else{
        $err = "Error:" . mysqli_error($mysqli);
        echo $err;
    }
}else{
    $err = "Error:" . mysqli_error($stmt);
    echo $err;
}
```

Obrázek 26 - Kód pro zápis průchodů do databáze

4.3.2. Arduino webový editor

Jak již bylo řečeno, prototyp má dvě řídící desky Wemos D1 Mini. Do každé s těchto desek bylo implementováno jedno softwarové řešení. Tyto dva software byly psány ve webovém editoru prostředí Arduino IDE, které je volně dostupné skrze Arduino Cloud na adrese https://create.arduino.cc/editor.

Prvním nezbytným krokem bylo stažení knihovny *ArduinoJson.h* pro práci s řídícími deskami. Dalším krokem byla instalace originálního programu *ArduinoCreateAgent*. Ten je prostředníkem mezi Arduino webovým editorem a počítačem uživatele. Pomocí něj lze výsledný software nahrát do příslušné řídící desky.

V okamžiku, kdy je prostředí plně připraveno ke spuštění, přichází na řadu samotný software. Pro každou funkci prototypu je navržen samostatný software. Tyto dva software jsou obsaženy v rámci dvou souborů: *Laser_Gate.ino* a *Wifi_Sniffer.ino*. Každý s těchto souboru obsahuje podsoubor *config.h*, ve kterém jsou mimo jiné definovány veškeré základní proměnné, se kterými se následně dále pracuje. Jedná se převážně o definování proměnných pro připojení k předem určené WiFi síti, skrze kterou se prototyp bude připojovat k internetu kvůli odeslání nasbíraných dat. Dále definuje proměnné pro nastavení API, které slouží právě ke zmíněnému předání dat mezi prototypem a webovou aplikací.

```
1  // Define enum of type of passage (in/out)
2  enum coming {in, out};
3  const char* cominStr[] = {"in", "out"};
4  void sendData(int count = 0, coming passagee = in);
5
6  // Pins
7  #define CONFIG_OUT_GATE_PIN 4
8  #define CONFIG_IN_GATE_PIN 5
9
10 // WiFi
11 #define CONFIG_WIFI_SSID "yourWifiName"
12 #define CONFIG_WIFI_PASS "yourWifiPassword"
13
14 // API
15 #define CONFIG_ROOM "test_room"
16 #define CONFIG_TOKEN "nice"
17 #define CONFIG_BASE_URL ".../gate.php"
18
19 // Time until person reach second gate
20 #define CONFIG_TIME_DELAY 1000
21
22 // Enables Serial and print statements
23 #define CONFIG_DEBUG true
```

Obrázek 27 - Soubor config.h pro Laser gate

Proces odeslání datpro oba softwary je takřka identický. Nejprve dojde k připojení k síti WiFi, následně je vytvořen klient, do kterého se definuje hlavička. Součástí souboru je token sloužící k zabezpečení komunikace. V poslední řadě se vytvoří soubor JSON se všemi informacemi, který je následně skrze metodu POST odeslán do souboru *gate.php* nebo *mac.php*.

```
//Check WiFi connection status
if (WiFi.status() == WL_CONNECTED) {
  WiFiClient client;
  HTTPClient http;

  // Your Domain name with URL path or IP address with path
  http.begin(client, CONFIG_BASE_URL);
  http.addHeader("Content-Type", "application/json");
  http.addHeader("TOKEN", CONFIG_TOKEN);

  // Send HTTP POST request
  int httpResponseCode = http.POST(json);
```

Obrázek 28 - Funkce odeslání dat (WiFi sniffer)

Další část kódu, která stojí za zmínění, je proces monitorování všech WiFi kanálů v okolí. Toto je funkce WiFi snifferu, která neustále skenuje všech 15 kanálů. Jakmile dojde k oskenování všech kanálů, vytvoří se JSON dokument s nasbíranými informacemi.

```
//setup device to search for mac adress
setup_sniffer();

// Move thrue 15 channels
channel = 1;
wifi_set_channel(channel);
while (true) {
  nothing_new++;
  if (nothing_new > 200) {
    nothing_new = 0;
    channel++;
    if (channel == 15) break;
    wifi_set_channel(channel);
  }
  delay(1);
}
```

Obrázek 29 - Funkce skenování WiFi kanálů

Proces zjištění MAC adres je následující. Měřená data jsou získáváná v bitovém formátu, která jsou následně převedena do číselného formátu. Tento proces je aplikován pro získání MAC adres, MAC adres přístupových bodů a hodnoty rssi.

```
49    // For loop all find clients
50    for (int f = 0; f < clients_known_count; f++) {
51      clientinfo ci = clients_known[f];
52
53      // If client not empty or corupt
54      if (ci.err == 0 || ci.rssi != 0) {
55        skip = false;
56
57        // Create client object and fill data
58        JsonObject object = array.createNestedObject();
59        object["room"] = CONFIG_ROOM;
60
61        // Mac adress is saved like array of byts
62        String mac = "";
63        for (int i = 0; i < 6; i++) {
64          mac = mac + ci.station[i];
65        }
66        object["mac"] = mac;
67
68        // Mac adress is saved like array of byts
69        String ap_mac = "";
70        for (int i = 0; i < 6; i++) {
71          ap_mac = ap_mac + ci.ap[i];
72        }
73        object["ap_mac"] = ap_mac;
74        object["rssi"] = ci.rssi;
```

Obrázek 30 - Funkce získání MAC adres

V poslední řadě je nutné říct, že uvedený software pro WiFi sniffer je vyvinutý na základě open source projektu s názvem *Wifi-Sniffer-using-esp8266-and-arduino-ide*. Vytvořený software tedy není napsán kompletně nově pro potřeby této diplomové práce.

Pro správně fungování paprskové virtuální závory byla vytvořena funkce přičítání a odečítání průchodů. Funkce nejprve zjistí, zda došlo k sepnutí vstupního či výstupního čidla. Následně vypíše hlášku *Income 1/2* a dojde k přičtení hodnoty 1. V případě, že sepne jako první výstupní čidlo, vypíše se hláška *Outcome 1/2* a odečte se hodnota 1.

```
55  // Incaming counter
56  // If first gate is reach
57  if (digitalRead(CONFIG_IN_GATE_PIN) ) {
58      Serial.println("Income 1/2");
59
60    // Variable to count leinght of walkthru measurements
61    int time = 1;
62    // Try to read data from secon gate for 'CONFIG_TIME_DELAY' (read next comment)
63    while (time < CONFIG_TIME_DELAY) {
64      delay(1);
65      // and if gate is reach
66      if (digitalRead(CONFIG_OUT_GATE_PIN)) {
67        Serial.println("Income 2/2");
68        // send data to server
69        sendData(1, in);
70        loop();
71      }
72      time = time + 1;
73    }
74  }
```

Obrázek 31 - Funkce detekce příchodů

4.3.3. Databázový prostředí

Databázové prostředí je v rámci diplomové práce zpracováno v rámci webové aplikace phpmyadmin. Aplikace je určena pro správu relačních databází MySQL pomocí webového prohlížeče. Tato aplikace umožňuje vytvářet, mazat, upravovat a spravovat databáze, tabulky, sloupce, řádky, indexy, uživatele nebo přístupy k nim. Aplikace phpmyadmin dále poskytuje uživatelské rozhraní pro provádění různých SQL dotazů, import a export dat a mnoho dalších funkcí.

V rámci tohoto databázového prostředí byly vytvořeny dvě relační tabulky obsahující sebraná data z navrženého HW prototypu. První tabulka s názvem *connectedMac* slouží k uchování dat z WiFi snifferu. Tabulka je rozdělena celkem na 8 sloupců. Hlavička tabulky v databázi vypadá tedy následovně:

id	mac	ap_ssid	channel	ap_mac	rssi	date	room

Tabulka 1 - Hlavička relační tabulky connectedMac

Sloupec *id* je unikátním identifikátorem jednotlivých záznamů v tabulce. Sloupec *mac* obsahuje konkrétní sebrané mac adresy z okolních zařízení. Sloupec *ap_ssid* obsahuje název WiFi, ze které se zařízení připojuje. Sloupec *channel* označuje kanál, skrze který komunikuje. Sloupec *ap_mac* definuje mac adresu přístupového bodu. Sloupec *rssi* je indikátor intenzity signálu (více než -73 dBm = velmi dobrý, od -75 dBm do -85 dBm = dobrý, od -87 dBm do -93 dBm = špatný, méně než -95 dBm = velmi špatný). Sloupec *date* představuje konkrétní datum a čas, kdy byl záznam v tabulce vytvořen. Posledním sloupcem v této tabulce je *room*, který je zde spíše jako možnost pro budoucí rozšíření prototypu do více místností. V současné době se s tímto řádkem nikterak nepracuje.

Druhá vytvořená relační tabulka v databázi je pojmenována *passage*. Ta obsahuje nasbírané hodnoty z paprskové závory. Jedná se tady o průchody (příchody a odchody). Tato relační tabulkou je rozdělena na 5 sloupců. Hlavička tabulky v databázi vypadá tedy následovně:

id	date	type	count	room

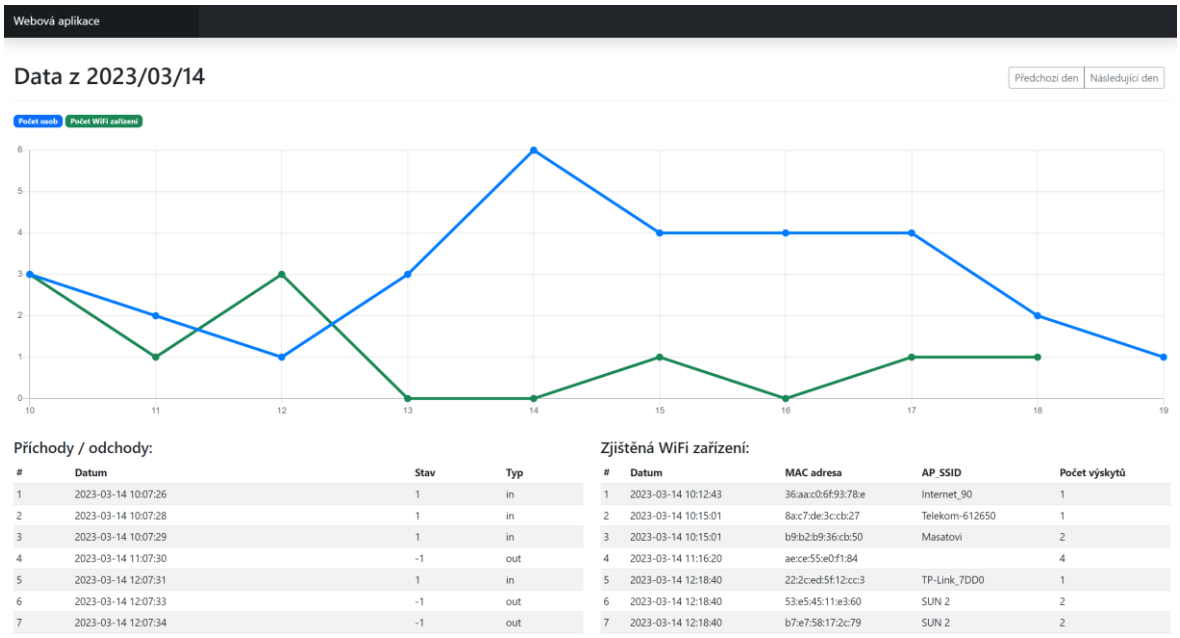
Tabulka 2 - Hlavička relační tabulky passage

Sloupec *id* je zde opět unikátním identifikátorem jednotlivých záznamů pro danou tabulku. Sloupec *date* představuje konkrétní datum a čas, kdy byl záznam v tabulce vytvořen. Sloupec *type* může nabývat celkem dvou hodnot: IN, OUT. Určuje tedy typ záznamu, zda se jedná o příchod osoby do místnosti nebo odchod. Sloupec *count* nabývá taktéž dvou hodnot: 1, -1. Slouží tedy k zjištění počtu osob v místnosti. Posledním sloupcem v této tabulce je *room*, který je zde spíše jako možnost pro budoucí rozšíření prototypu do více místností. V současné době se s tímto řádkem nikterak nepracuje.

4.4. Vizualizace dat

Vizualizace dat je zprostředkována skrze výstup webové aplikace. Aplikace je rozdělena do 3 základních bloků. V hlavičce stránky nalezneme informaci, ze kterého dne

jsou data vizualizována. Dny lze jednoduše přepínat pomocí přepínače vpravo nahoře. Primární částí aplikace je graf znázorňující nasbírané hodnoty po jednotlivých hodinách. V grafu se nacházejí dvě křivky, které zaznamenávají hodnoty a jak se v čase vyvíjejí. Modrá křivka představuje počet zaznamenaných osob (tedy počet příchodů – počet odchodů). Zelená křivka udává počet unikátních MAC adres v okolí. Pod grafem se zobrazují dvě tabulky s konkrétními naměřenými hodnotami. Tabulka vlevo vypisuje hodnoty příchodů a odchodů, konkrétně datum a čas záznamu průchodu, stav změny a typ průchodu. Tabulka vpravo vypisuje data ohledně získaných zařízení s aktivním WiFi adaptérem v okolí. Konkrétně tedy opět datum a čas záznamu, MAC adresu, název WiFi sítě, skrze kterou se zařízení připojuje (AP_SSID) a počet kolikrát se daná MAC adresa nachází v databázi (kolikrát je celkem v daný den zaznamenaná).



#	Datum	Stav	Typ
1	2023-03-14 10:07:26	1	in
2	2023-03-14 10:07:28	1	in
3	2023-03-14 10:07:29	1	in
4	2023-03-14 11:07:30	-1	out
5	2023-03-14 12:07:31	1	in
6	2023-03-14 12:07:33	-1	out
7	2023-03-14 12:07:34	-1	out

#	Datum	MAC adresa	AP_SSID	Počet výskytů
1	2023-03-14 10:12:43	36:aa:c0:6f:93:78:e	Internet_90	1
2	2023-03-14 10:15:01	8a:c7:de:3c:cb:27	Telekom-612650	1
3	2023-03-14 10:15:01	b9:b2:b9:36:cb:50	Masatovi	2
4	2023-03-14 11:16:20	ae:ce:55:e0:f1:84		4
5	2023-03-14 12:18:40	22:2ced:5f:12:cc:3	TP-Link_7DD0	1
6	2023-03-14 12:18:40	53:e5:45:11:e3:60	SUN 2	2
7	2023-03-14 12:18:40	b7:e7:58:17:2c:79	SUN 2	2

Obrázek 32 - Ukázka webové aplikace

4.5. Testování

V této kapitole podrobněji rozebereme postup spuštění a následného testování nově sestrojeného prototypu. V první fázi testování byl kladen důraz na obecnou funkčnost prototypu. Sledován byl primárně proces správného přenosu dat z HW prototypu do databáze skrze vytvořené API. Dalším sledovaným bodem byl výpis dat. Jelikož se data

vypisují do grafů po hodinách, bylo důležité podrobně otestovat správnost vypisovaných dat. Tyto data jsou selektována pomocí poměrně složitých SQL dotazů, tudíž bylo nutné zjistit, zda jsou vybraná data relevantní.

Během dalšího testování bylo odhaleno několik následujících chyb či nedostatků. První zjištěnou chybou byl nekorektní formát zápisu času do databáze. Bylo zjištěno, že databázové prostředí použité pro účely testování prototypu má jako výchozí nastavení časové pásmo GMT+0. To mělo za následek chybně zapsané hodnoty. Čas byl posunut o hodinu zpět, jelikož Česká republika se nachází v časovém pásmu GMT+1. Bohužel databázové prostřední nenabízí možnost změny časového pásma, bylo tedy definovat časový formát přímo v souborech *mac.php* a *gate.php*, které zajišťují API. Datum a čas není definován až databází, ale již při odesílání skrze PHP, čímž byl problém trvale vyřešen.

Další nečekaným zjištěním bylo, že při odesílání dat z WiFi snifferu do databáze, se MAC adresy odesílají ve špatném formátu (v desetinné číselné soustavě). V rámci Arduino webového editoru dochází ke zjištění MAC adres po jednotlivých bitech. Tyto bity se, ale automaticky zapisují v desetinné číselné soustavě, čímž byl odhalen zdroj problému. Bylo tedy nutné zajistit správný formát MAC adresy na straně PHP. Před odesláním dat do databáze provede PHP následnou transformaci dat. Převede data z desetinné číselné soustavy do hexadecimální, dále vytvoří pole *array* a data rozdělní po 2 znacích, mezi každý druhý znak vloží dvojtečku a v posledním kroku celé pole opět spojí do jedné proměnné, která se odešle do databáze jako MAC adresa zjištěného zařízení.

Při testování virtuální paprskové závory byl zjištěn problém se samovolným zaznamenáváním příchodů, aniž by nastal jakýkoli pohyb vně závory, a to i po několika pokusech o seřízení dražšího z dvojice senzorů (stavebnice, viz Obrázek 16). Ačkoli by tento dražší senzor měl být odolnější vůči okolním vlivům, tak tyto specifika se nepotvrdily. Senzor byl nakonec nahrazen druhým levnějším typem paprskového senzoru, který funguje výrazně přesněji.

Dalším zjištěním bylo, že při výpisu dvou křivek do grafu (hodnot průchodů a naměřených MAC adres) skript, který se stará o výpis dat, neví, jakou časovou osu pro graf nastavit, jelikož každá křivka má přiřazené své časové hodnoty pro tuto osu. Došlo k vytvoření procedury, která v případě dvou křivek v grafu zjistí nejnižší a nejvyšší

naměřenou hodinu v rámci obou křivek. Na základě těchto dvou hodnot následně sestaví časovou osu.

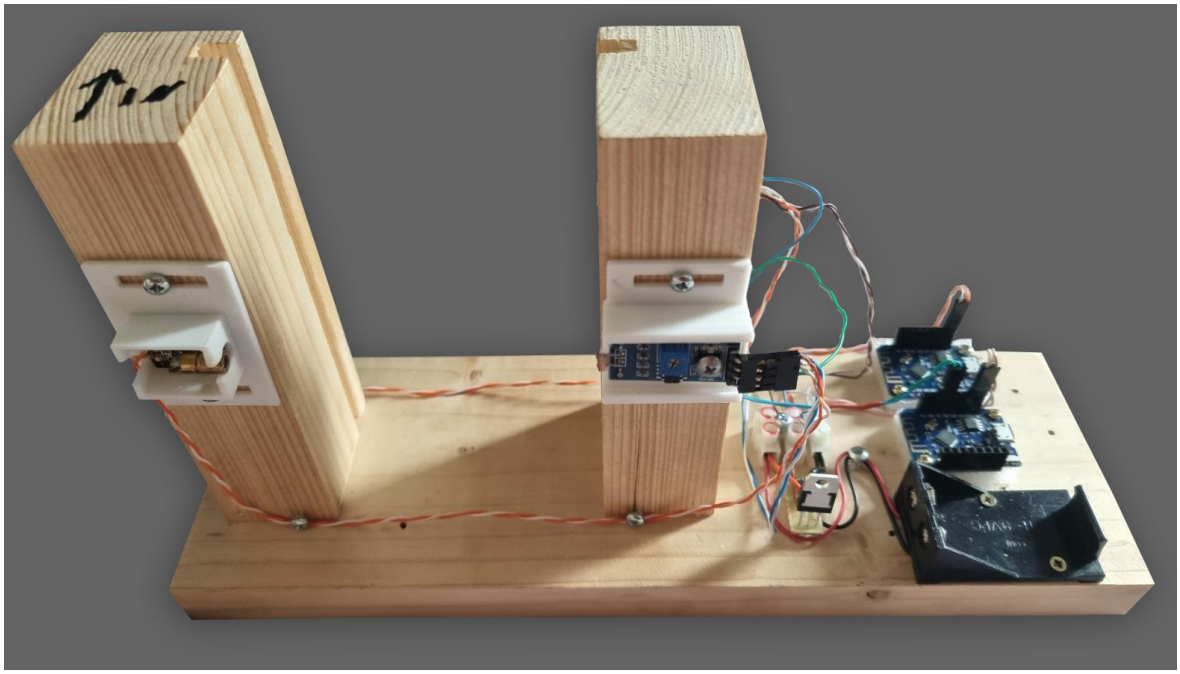
V poslední řadě byl odhalen problém při vizualizaci dat v grafu v rámci webové aplikace. Problém nebyl trvalý, ale nastával jen ve specifických situacích, které se pomocí testování prototypu podařilo správně odhalit. Problém spočíval v situaci, kdy v rámci časové osy grafu nebylo v některou hodinu nic naměřeno. Hodnota pro tuto hodinu byla tedy prázdná, čímž došlo k posunutí následných hodnot o hodinu zpět (v případě pouze jedné hodiny, ve které nebylo nic naměřeno). Bylo tedy nutné upravit funkce *getUniqMacGraphData* a *getPassageGraphData* tak, aby v těchto specifických situacích hodnoty dopočítaly a zabránily nežádoucímu posunu hodnot v grafu. V případě funkce *getUniqMacGraphData* dochází při nenaměřené hodině k zapsání hodnoty 0, pro danou hodinu. Naopak v případě funkce *getPassageGraphData* je zapotřebí zapsat hodnotu z poslední předchozí naměřené hodiny, protože nedošlo k žádnému průchodu senzorem, je tedy nutné zapsat stejný počet osob, jelikož nikdo nepřišel ani neodešel, tak se počet osob v místnosti nezměnil.

5. Výsledky a diskuse

Vlastní práce spočívala v seznámení čtenáře o procesu zpracování nově navrženého řešení dle nastudovaných poznatků z teoretické části diplomové práce. Čtenář byl seznámen s jednotlivými kroky vývoje, postupy práce a použitým HW a SW. Na základě těchto sdělení bude čtenář v této kapitole seznámen s konkrétními fyzickými výstupy, cenovým rozpočtem na použitý hardware a v poslední řadě bude seznámen s možným budoucím vývojem monitorování osob.

5.1. Výsledný prototyp

Fyzickým výstupem této diplomové práce je nově sestrojený HW prototyp, který má za úkol shromažďovat data ze svého okolí a tím rozšiřovat datovou základnu pro následnou interpretaci výsledků a výstupů prováděné studie.



Obrázek 33 - Výsledný HW prototyp

Na Obrázek 33 lze vidět finální podobu zmiňovaného HW prototypu. V pravé části obrázku jsou patrné dvě řídící desky Wemos D1 mini (clone), ve kterých je implementovaný

vyvinutý software. Deska výše (z pohledu obrázku) obsahuje software pro WiFi sniffer, deska pod ní pro virtuální závoru. Z důvodu nasimulování vstupní brány je vytvořen na dřevěné desce průchodový bod. Z každé strany (vstupní i výstupní) jsou umístěny dva senzory – laserový modul a digitální světelný senzor, které průchody zaznamenávají.

5.1.1. Cenový rozpočet materiálu

V této kapitole je podrobně rozepsaný seznam potřebného HW materiálu s jeho cenami, který byl potřeba k sestrojení nového prototypu. Celková cena součástek činí 995 Kč. V případě domácího sestavení či jiného využití není nutné se bát počátečních nákladů. Co je zde však dobře patrné, je rozdíl cen mezi paprskovou závorou (stavebnice) a součtem laserového modulu s digitálním světelným senzorem. Rozdíl je 485 Kč za téměř identické součástky. Odpověď tedy na výše zmíněnou otázku, jaký je rozdíl funkcionality mezi těmito dvěma druhy paprskových závor, hraje ve prospěch levnější varianty.

Název součástky	**Cena**
2x Wemos D1 mini (clone)	240 Kč
Paprsková závora (stavebnice)	535 Kč
Laserový modul	20 Kč
Digitální světelný senzor	30 Kč
Regulátor napětí	10 Kč
Napájecí baterie 5 V	70 Kč
Držák napájecí baterie 30 Kč	30 Kč
Ostatní materiál (dráty, konektory, …)	60 Kč

Tabulka 3 - Cenový rozpočet prototypu

5.2. Možnosti budoucího vývoje monitoringu budov

Do budoucna je očekávaný vývoj vylepšených senzorů. Senzory, které jsou nyní k dispozici pro monitorování osob v budově, se stále zdokonalují a vylepšují. Například senzory pro sledování pohybu mohou být vylepšeny tak, aby mohly rozpoznat individuální osoby podle jejich chůze, nebo aby mohly určit, jestli se někdo pohybuje podezřelou rychlostí. Senzory pro měření teploty mohou být vylepšeny tak, aby byly schopny měřit teplotu většího počtu osob najednou a poskytovaly tak mnohem větší a komplexnější množství dat.

Dále je velmi očekávané rozsáhlejší využití umělé inteligence. Umělá inteligence může být v budoucnu využita k lepšímu zpracování a analýze dat v monitorovaných oblastech. Například by mohla být využita k rozpoznání individuálních osob z obrazových záznamů a k vytvoření profilu jejich chování v budově.

V budoucnu by mohly být různé senzory a technologie sloučeny do jednoho integrovaného systému, který by mohl poskytovat mnohem komplexnější a přesnější data o pohybu osob v budově. Například by mohl být vytvořen systém, který by kombinoval senzory pro měření teploty, pohybu a kvality ovzduší, aby poskytoval komplexní informace o podmínkách v budově. Zároveň může být kladen větší důraz na ochranu soukromí osob v budově a na omezení sběru a zpracování dat. Tudíž mohou být vytvořeny nové technologie, které by umožnily anonymní sběr dat, anebo by mohly být využity technologie šifrování dat, aby byla zajištěna jejich bezpečnost.

V neposlední řadě se očekává velký rozvoj chytrých zařízení. V následujících letech by mohla být využita chytrá zařízení, jako jsou například chytré hodinky, brýle nebo jiné nositelné technologie, k získávání dat o pohybu osob v budově. Tyto zařízení by mohla být využita k vytváření mnohem detailnějších profilů chování osob v budově.

6. Závěr

Cílem této diplomové práce, která je zaměřena na problematiku monitoringu osob uvnitř budov s využitím zařízení internetu věci, bylo správně analyzovat stávající řešení, navrhnout vhodné možnosti, jak toto řešení rozšířit a tím i zpřesnit stávající systém monitoringu. Následně sestrojit vlastní prototyp s funkcemi stávajícího řešení a implementovaným navrženým rozšířením.

Prvním krokem vlastní práce bylo provedení analýzy stávajícího řešení, čímž je diplomová práce Ing. Jana Poláčka na téma „Využití internetu věcí pro monitoring obsazenosti budov“. Jeho řešení volně vychází ze systému WOLNO, který je aktivně využíván na Provozně ekonomické fakultně České zemědělské univerzity v Praze. Analýzou bylo zjištěno, že hlavní nevýhodou stávajícího řešení je skutečnost, že zařízení vždy musí mít aktivní WiFi adaptér, aby mohla být detekována. Sekundárním problémem je i fakt, že pomocí tohoto řešení je možné docílit pouze přesného počtu zařízení (sčítáním MAC adres) a následně se pokusit o odhad počtu osob.

Na základě tohoto zjištění bylo navrženo vhodné rozšíření. Prvotně myšleným rozšířením byla možnost detekce zařízení skrze Bluetooth. Tím by však nebylo možné docílit přesného počtu osob a zároveň by přetrval problém nutnosti mít zapnutý Bluetooth adaptér. Závěrem bylo rozhodnuto, že Bluetooth není vhodné použít jako rozšíření stávajícího řešení, jelikož by rozšíření nemělo dostatečnou přidanou hodnotu. Vhodnou variantou byla implementace paprskové virtuální závory, která zaznamenává průchody vně senzoru. Tímto způsobem lze docílit přesného počtu osob v dané lokaci. Což je absolutní řešení primárního a sekundárního problému z předešlé analýzy. Za předpokladu, že každé nositelné zařízení nemá aktivní WiFi adaptér je navržená paprsková virtuální závora vhodným rozšířením, se kterým lze lokaci monitorovat i bez aktivního WiFi či Bluetooth adaptéru.

Následné kroky spočívaly v sestrojení HW prototypu pomocí vhodně vybraných součástek internetu věcí a ve vývoji několika SW řešení pro účely sběru, uchování a vizualizaci naměřených pozičních dat. Jako HW řídící vývojová deska byla vybrána destička s označením Wemos D1 mini (clone), která obsahuje WiFi modul ESP8266, splňuje potřebné

parametry k užití a zároveň je uživatelsky přívětivějším řešením díky obsaženému micro USB slotu. Oproti samostatnému čipu ESP8266, který žádný USB slot nemá a musí se použít převaděč.

V rámci testování prototypu bylo mimo jiné odhaleno samovolné zaznamenávání příchodů na straně příchozího paprskového senzoru. Senzor byl nakonec nahrazen levnějším typem paprskového senzoru použitým na odchozí straně, který funguje výrazně přesněji. Čímž bylo zároveň odpovězeno na otázku, zda existují mezi těmito dvěma typy senzorů zásadní rozdíly ve funkčnosti, což byl sekundární důvod použití dvou rozdílných typů senzorů. Ačkoli tento příchodový senzor byl dražší a měl být odolnější vůči okolním vlivům, tak se tyto jeho specifikace nepotvrdily.

Navržený prototyp tedy rozšiřuje datový sklad o nový pohled na data. Jelikož je schopen měřit dva odlišné druhy informací, napomáhá k zpřesnění měření a následných výstupů monitorování. V případě budoucího použití monitorování pouze pomocí WiFi snifferu, lze na základě dat o průchodech vypočítat průměrnou odchylku měření MAC adres, čímž se následně více přiblížit přesnému počtu osob ve sledovaném prostoru při absenci virtuální paprskové závory.

7. Seznam použitých zdrojů

[1] K. Foote, “A Brief History of the Internet of Things,” 14 Leden 2022. [Online]. Available: https://www.dataversity.net/brief-history-internet-things/.

[2] P. Peranzo, “8 Sectors That Can Benefit the Most from IoT Development,” 1 Listopad 2022. [Online]. Available: https://imaginovation.net/blog/8-sectors-benefit-from-iot-development-in-2021/.

[3] S. Al-Sarawi, M. Anbar, K. Alieyan a M. Alzubaidi, Internet of Things (IoT) communication protocols, IEEE, 2017.

[4] C. BasuMallick, „What is IPv6: Important Features and Uses,“ 6 Říjen 2022. [Online]. Available: https://www.spiceworks.com/tech/networking/articles/what-is-ipv6/.

[5] G. Acosta, „The ZigBee Protocol,“ 26 Březen 2018. [Online]. Available: https://www.netguru.com/blog/the-zigbee-protocol.

[6] Bluetooth, „Bluetooth Technology Overview,“ 1 2023. [Online]. Available: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/.

[7] S. Shea, „Z-Wave,“ Srpen 2018. [Online]. Available: https://www.techtarget.com/iotagenda/definition/Z-Wave.

[8] Advanced NFC, „Near field communication overview,“ 16 Květen 2022. [Online]. Available: https://developer.android.com/guide/topics/connectivity/nfc.

[9] P. Holešinský, Výzkum lokalizačních algoritmů pro bezdrátové senzorové sítě, Brno, 2009.

[10] A. Froehlich, „What is a Location-Based Service and How Does It Work?,“ 2018. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/location-based-service-LBS.

[11] Novatel, „What is GPS?,“ 2019. [Online]. Available: https://novatel.com/support/knowledge-and-learning/what-is-gps-gnss.

[12] D. Zhang, F. Xia, Z. Yang, L. Yao a W. Zhao, Localization Technologies for Indoor Human Tracking, IEEE, 2010.

[13] K. Cunningham, „Map Triangulation,“ 26 Duben 2022. [Online]. Available: https://www.myopencountry.com/how-to-triangulate-map/.

[14] C. Laoudias, A. Moreira, S. Kim, S. Lee, L. Wirola a C. Fischione, A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation, IEEE, 2018.

[15] J. Poláček, Využití internetu věcí pro monitoring obsazenosti budov, Praha, 2022.

[16] e-education, „Trilateration,“ 2020. [Online]. Available: https://www.e-education.psu.edu/natureofgeoinfo/c5_p12.html.

[17] czwiki, „Trilaterace,“ 15 Leden 2022. [Online]. Available: https://czwiki.cz/Lexikon/Trilaterace.

[18] occuspace, „Occupancy Monitoring,“ 15 1 2023. [Online]. Available: https://occuspace.io/blog/occupancy-monitoring-101.

[19] gdpr, „What is GDPR, the EU’s new data protection law?,“ 1 2023. [Online]. Available: https://gdpr.eu/what-is-gdpr/.

[20] Verizon, „What is Wi-Fi?,“ 28 Červenec 2022. [Online]. Available: https://www.verizon.com/articles/internet-essentials/wifi-definiton/.

[21] KIT, „Obsazenost areálu ČZU,“ 2020. [Online]. Available: https://ls40.pef.czu.cz/obsazenost-arealu-czu.

[22] Samsung, „What is Bluetooth and how do i use it?,“ 2022. [Online]. Available: https://www.samsung.com/uk/support/mobile-devices/what-is-bluetooth/.

[23] E. Nesbo, „What Is BLE (Bluetooth Low Energy),“ 27 Prosinec 2021. [Online]. Available: https://www.makeuseof.com/what-is-ble-bluetooth-low-energy/.

[24] R. Murshed, „Find all Bluetooth devices (headsets, phones etc) nearby, without forcing the devices in discoverable mode,“ 2 Květen 2016. [Online]. Available: https://stackoverflow.com/questions/35239880/find-all-bluetooth-devices-headsets-phones-etc-nearby-without-forcing-the-de.

[25] V-count, „People Counting Technologies,“ 19 Listopad 2021. [Online]. Available: https://v-count.com/people-counting-technologies-a-comprehensive-guide/.

[26] C. Wadsworth, „People Counting Technology,“ 1 Únor 2018. [Online]. Available: https://www.trafsys.com/how-to-choose-a-people-counting-solution/.

[27] Y. Choudhary, „Top 15 IoT Sensor Types and How Development Companies Use Them,“ [Online]. Available: https://www.finoit.com/blog/top-15-sensor-types-used-iot/.

[28] C. Kolade, „What is HTML - Definition and Meaning,“ 24 Srpen 2021. [Online]. Available: https://www.freecodecamp.org/news/what-is-html-definition-and-meaning/.

[29] B. Artūras, „What is CSS,“ 4 1 2023. [Online]. Available: https://www.hostinger.com/tutorials/what-is-css.

[30] Arduino, „Arduino Integrated Development Environment,“ 15 Prosinec 2022. [Online]. Available: https://docs.arduino.cc/software/ide-v1/tutorials/arduino-ide-v1-basics.

[31] Cisco, „What Is a Wireless LAN?,“ 1 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/wireless/wireless-lan.html.

[32] SamB, „Wireless Local Area Network (WLAN) - Architecture,“ 5 Březen 2022. [Online]. Available: https://forum.huawei.com/enterprise/en/wireless-local-area-network-wlan-architecture/thread/833939-869.

[33] MySQL, „What is MySQL?,“ 1 2023. [Online]. Available: https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html.

[34] A. Krishna and A. Singh, Internet of Things & Wireless Sensor Network, 2019.

[35] Y. Li, J. Barthelemy, S. Sun, P. Parez and B. Morgan, A Case Study of WiFi Sniffing Performance Evaluation, IEEE, 2020.

[36] J. Kurose, Počítačové sítě, Brno: Computer Press, 2014.

[37] G. Colbach, Wireless Networking: Introduction to Bluetooth and WiFi, 2017.

[38] E. Vattapparamban, B. Ciftler, İ. Güvenc, K. Akkaya and A. Kadri, Indoor occupancy tracking in smart buildings using passive sniffing of probe requests, IEEE, 2016.

[39] S. Astari, „What is PHP,“ 1 Březen 2013. [Online]. Available: https://www.hostinger.com/tutorials/what-is-php/.

8. Seznam obrázků, tabulek a zkratek

8.1. Seznam obrázků

Obrázek 1 - Přehled vlastností ZigBee oproti jiným protokolům 18
Obrázek 2 - Schéma architektury GNSS 22
Obrázek 3 - Schéma triangulace 25
Obrázek 4 - Schéma proximity 26
Obrázek 5 - Schéma trilaterace 26
Obrázek 6 - Rozhraní aplikace WOLNO 32
Obrázek 7 - Schéma komunikace BLE 33
Obrázek 8 - Paprskový senzor 36
Obrázek 9 - Tepelný senzor 37
Obrázek 10 - Time-of-Flight senzor 38
Obrázek 11 - 2D Mono senzor 39
Obrázek 12 - 3D stereo senzor 40
Obrázek 13 - Schéma architektury WLAN 46
Obrázek 14 - Logo systému WOLNO 49
Obrázek 15 - Wemos D1 Mini (clone) 52
Obrázek 16 - Paprsková závora (stavebnice) 53
Obrázek 17 - Laserový modul 54
Obrázek 18 - Digitální světelný senzor 55
Obrázek 19 - Napájecí baterie 9 V 55
Obrázek 20 - Funkce createDbConnection 57
Obrázek 21 - Funkce getPassageTable 57
Obrázek 22 - Funkce getPassageGraphData 58
Obrázek 23 - Funkce getUniqMacTable 59
Obrázek 24 - Funkce getUniqMacGraphData 60
Obrázek 25 - Kód pro zápis MAC adres do databáze 61
Obrázek 26 - Kód pro zápis průchodů do databáze 61
Obrázek 27 - Soubor config.h pro Laser gate 62
Obrázek 28 - Funkce odeslání dat (WiFi sniffer) 63

Obrázek 29 - Funkce skenování WiFi kanálů 63
Obrázek 30 - Funkce získání MAC adres 64
Obrázek 31 - Funkce detekce příchodů 65
Obrázek 32 - Ukázka webové aplikace 67
Obrázek 33 - Výsledný HW prototyp 70

8.2. Seznam tabulek

Tabulka 1 - Hlavička relační tabulky connectedMac 65
Tabulka 2 - Hlavička relační tabulky passage 66
Tabulka 3 - Cenový rozpočet prototypu 71

8.3. Seznam zkratek

AP – *Access Point*

API – *Aplikační Softwarové Rozhraní*

ARPANET – *Advanced Research Projects Agency Network*

BLE – *Bluetooth Low Energy*

BSS – *Basic Service Set*

BT – *Bluetooth*

BTS – *Base Transceiver Station*

CGI – *Common Gateway Interface*

CSS – *Cascading Style Sheets*

GDPR – *General Data Protection Regulation*

GNSS – *Global Navigation Satellite Systems*

GPS – *Global Positioning Satellites*

HTML – *HyperText Markup Language*

HW – *Hardware*

IETF – *Internet Engineering Task Force*

IoT – *Internet of Things*

LBS – *Location Based Services*

NFC – *Near Field Communication*

PHP – *Personal Home Page*

SW – *Software*

ToF – *Time-of-Flight*

USB – *Universal Serial Bus*

WEP – *Wired Equivalent Privacy*

WiFi – *Wireless Fidelity*

WLAN – *Wireless Local-Area Network*

WPA – *WiFi Protected Access*

WSN – *Wireless Sensor Network*