Univerzita Pardubice

Fakulta ekonomicko-správní

Zabezpečení prostředků k získávání dat pro chytrá města

Jakub Ptáčník

Bakalářská práce

2018

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2017/2018**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jakub Ptáčník**
Osobní číslo:	**E15077**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Zabezpečení prostředků k získávání dat pro chytrá města**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je návrh zabezpečení vybraných senzorových a přenosových prostředků používaných k získávání dat pro chytrá města.

Osnova:
- Prostudování vybraných komunikačních technologií a senzorů
- Stanovení zranitelných míst
- Návrh způsobu zabezpečení vlastních senzorů a přenosových cest

Rozsah grafických prací:

Rozsah pracovní zprávy: **30 - 40 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

ALLWINKLE, Sam, CRUICKSHANK, Peter. Creating Smart-er Cities: An Overview. Journal of Urban Technology [online]. 2011, 18(2), 1-16 [cit. 2017-10-06]. DOI: 10.1080/10630732.2011.601103. ISSN 1063-0732. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/10630732.2011.601103

ENDORF, Carl F., MELLANDER, Jim, SCHULTZ, Eugene. Detekce a prevence počítačového útoku. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.

FOSTER, James C. Hacking - Buffer Overflow: [zneužití, detekce a prevence]. Praha: Grada, 2007, 348 s. ISBN 978-80-247-1480-6.

MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hacking bez záhad. Praha: Grada, 2007, 520 s. ISBN 978-80-247-1502-5.

Vedoucí bakalářské práce: **Mgr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2017**

Termín odevzdání bakalářské práce: **30. dubna 2018**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 1. září 2017

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 25.04. 2018 Jakub Ptáčník

PODĚKOVÁNÍ

Mé poděkování patří Mgr. Ing. Oldřichovi Horákovi, Ph.D., za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnoval.

ANOTACE

Tato bakalářská práce se zabývá problematikou kybernetických útoků na technologie a senzory konceptu Smart City. Autor stanovuje zranitelná místa použitých technologií a pomocí případové studie navrhuje bezpečnostní opatření, jejichž cílem je zabránit kybernetickému útoku. V závěru autor dává obecná doporučení pro vytvoření bezpečného návrhu Smart City.

KLÍČOVÁ SLOVA

Smart City, Internet of Things, bezpečnost, kybernetický útok, případová studie

TITLE

Securing Resources to Obtain Data for Smart Cities

ANNOTATION

This bachelor thesis deals with the problem of cyberattacks on Smart City technologies and sensors. Author determines security vulnerabilities of used technology and using a case study proposes a security measures to prevent a cyberattack. In conclusion, author gives general recommendations for creating safe and secure Smart City solution.

KEYWORDS

Smart City, Internet of Things, security, cyberattack, case study

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

CCTV – Closed Circuit Television

CDMA – Code Division Multiple Access

DDoS – Distributed Denial of Service

DoS – Denial of Service

EOP – Ethernet Over Power

GPRS – General Packet Radio Service

GSM – Global System for Mobile Communication

IoT – Internet of Things

LPWAN – Low Power Wide Area Network

LTE – Long Term Evolution

NFC – Near-Field Communication

SQL – Structured Query Language

UDP – User Datagram Protocol

Úvod

Termín chytrá města, případně anglický pojem Smart City, je v poslední době velmi diskutovaným tématem. Obecně lze říci, že chytré město je takové, které využívá informační a komunikační technologie připojené k síti. Mezi ně se řadí různé druhy senzorů sbírajících data, která jsou následně analyzována a použita k řízení zdrojů, optimalizaci každodenních činností a zefektivnění služeb, které jsou poskytovány občanům.

Používání zařízení a technologií, které jsou připojené k síti, ať za účelem vzdálené správy nebo pasivního odesílání dat, s sebou nese velká bezpečnostní rizika. Zejména při použití zmíněných technologií v kritické infrastruktuře měst, jakou je například doprava nebo energetická síť. Tyto systémy se mohou stát terčem kybernetických útoků. Při napadení kritické infrastruktury mohou vznikat závažné škody a v nejhorších případech mohou být ohroženy i lidské životy. Z toho důvodu je nezbytné se zabezpečením konceptu Smart City důkladně zabývat.

Tato práce má stanoveny tři konkrétní úkoly:

1. Prostudování vybraných komunikačních technologií a senzorů.
2. Stanovení zranitelných míst.
3. Návrh způsobu zabezpečení vybraných senzorů a přenosových cest.

První část práce je věnována definici konceptu Smart City, popisu používaných IoT technologií a vymezení pojmů. V druhé části jsou stanovena zranitelná místa, které může potenciální útočník využít a ohrozit tak bezpečnost celého systému. Poslední kapitola druhé části práce je věnována již zdokumentovaným útokům, které slouží pro demonstraci zranitelnosti konceptu Smart City a technologií Internetu věcí. V poslední části je uvedena případová studie s fiktivním městem, které používá vybrané technologie. Následně je navrženo zabezpečení těchto technologií, jejich senzorových prostředků a přenosových cest.

Cílem práce je identifikovat možnosti zneužití a navrhnout vhodná opatření, která zajistí bezpečné používání zařízení a technologií používaných v chytrých městech.

1 KOMUNIKAČNÍ TECHNOLOGIE KONCEPTU SMART CITY

V první řade je nasnadě položit si otázku: *Proč dělat město „chytré“?*

Více než polovina (54 %) aktuální světové populace žije ve městech. V 50. letech minulého století žilo v městských oblastech jen 30 % populace. V roce 2009 byla celková světová populace odhadnuta na 6,8 miliardy lidí, z toho 3,7 miliardy obývá města. Předpokládá se, že do roku 2050 bude 66 % populace žít ve městech [18]. Díky urbanizaci se tak do měst stěhuje více lidí a města se stávají většími. Stávající infrastruktura měst nemusí být připravena na tak rychlý rozmach urbanizace. To může zapříčinit zásadní neefektivnost v oblastech energetiky, dopravy, nakládání s odpadem atp. a současně hrozí i sociální problémy, například vznik slumů nebo rozptýlených pracovišť.

Veřejný i soukromý sektor proto investuje nemalé finanční částky do inteligentních technologií, aby našel řešení těchto sociálních, ekonomických a environmentálních problémů a zároveň nabídl lepší prostředí pro život. [2][33]

1.1 Definice konceptu Smart City

Koncept Smart City není úplnou novinkou a již nějakou dobu se vyvíjí. Samotná definice Smart City však neexistuje, koncept je vnímán z různých úhlů pohledu a současně se liší i názory některých odborníků.

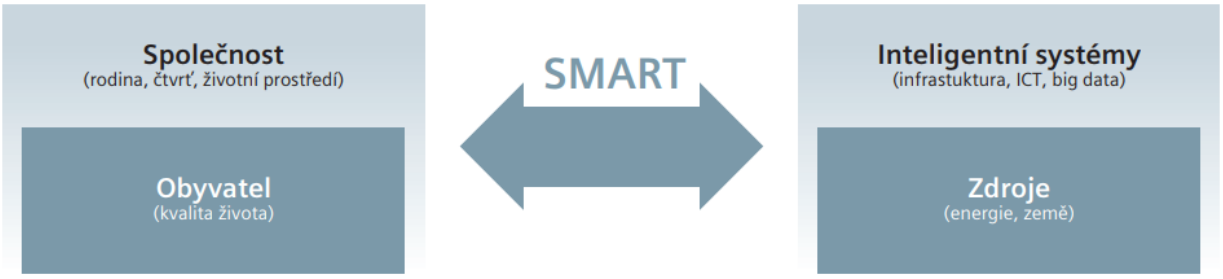
OSN definuje chytré město jako celek, který má vestavěné digitální technologie ve všech městských funkcích.

Podle děkana Dopravní fakulty ČVUT prof. Dr. Ing. Miroslava Svítka, dr. h. c., je potřeba význam slova „smart“ spatřovat ve vyvážené vazbě mezi člověkem a technickými systémy. Platí však, že chytrá řešení musejí činit města více humánními, ne pouze technologicky pokročilými. [17]

Základním kamenem konceptu Smart City je používání moderních technologií s důrazem na nízkou energetickou náročnost a vysokou kvalitu života. Mezi použité technologie lze zařadit téměř jakákoliv zařízení od fyzických detektorů až po komplexní informační systémy. Koncept také využívá a kombinuje infrastrukturu Internetu věcí (IoT), Internetu služeb (IoS – Internet of Services) a Internetu lidí (IoP – Internet of People). Součástí měst a regionů

jsou také průmyslové objekty a výrobní závody, proto je třeba zmínit i systémy Průmyslu 4.0 (Industry 4.0). [2][17]

Obrázek 1 zobrazuje koncept chytrého města podle Miroslava Svítka, děkana Dopravní fakulty ČVUT .



Obrázek 1: Koncept chytrého města

Zdroj: [17]

1.2 Vymezení pojmů Smart City

V celém konceptu Smart City se lze setkat s mnoha odvětvími, v této kapitole budou popsány nejčastěji používané pojmy.

1.2.1 Smart Transportation

Chytrá doprava a dopravní infrastruktura řeší problémy v řízení dopravy a mobility ve městech. Stále se zvyšující počet automobilů má za následek vysokou hustotu dopravy a vznik komplikovaných situací v přeplněných centrech měst. Problémům souvisejících s dopravou dnes čelí většina regionů a ve většině případů platí přímá úměra – čím větší město, tím komplikovanější dopravní situace (zejména v časech tzv. dopravní špičky).

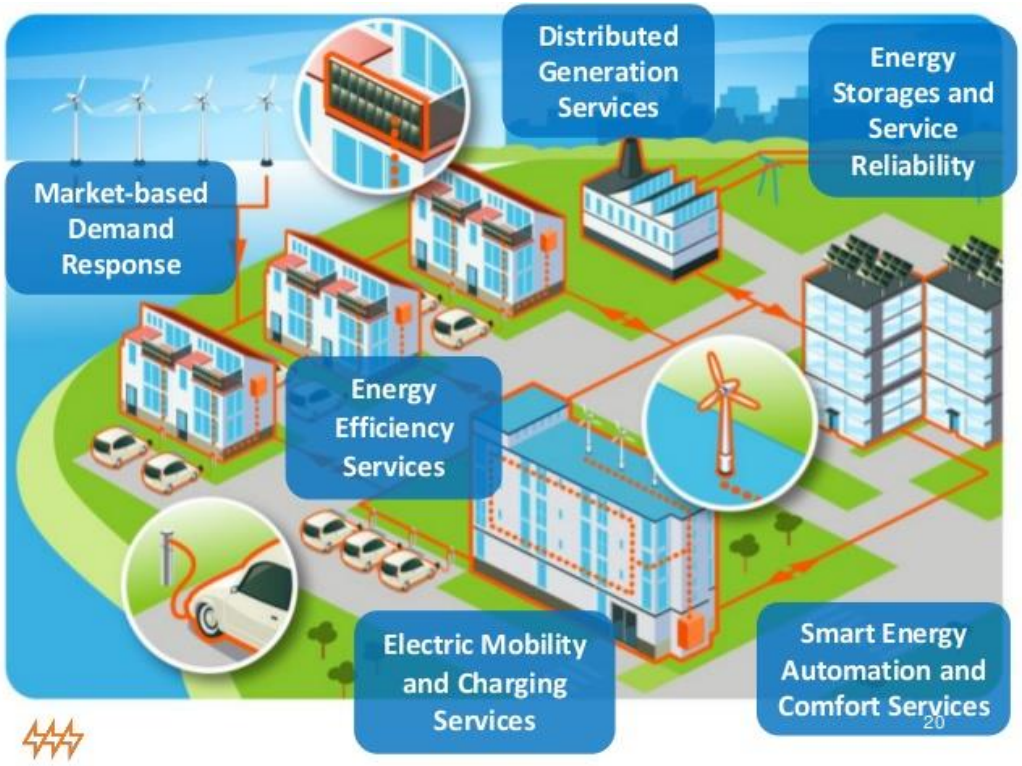
Občan České republiky průměrně ujede cca 18 km osobním automobilem, z této vzdálenosti připadají přibližně 4 km na hledání volného parkovacího místa. To vede ke zvyšování emisí CO_2 a NOx, a vyšší spotřebě paliva. [17]

Použitím vhodných technologií lze optimalizovat trasy vozidel městské hromadné dopravy, monitorovat volná parkovací místa a regulovat dopravní situaci ve městě tak, aby se omezily dopravní zácpy.

1.2.2 Smart Energy

Mezi cíle inteligentní energie patří zlepšení efektivity používaných zdrojů, automatizace energetického řídicího systému a uskladňování nevyužité energie.

S oblastí energetiky také úzce souvisí koncept Smart Grids (viz Obrázek 2), čili chytré sítě (např. elektrické). Použitím digitálních technologií v síti dochází k obousměrnému propojení a komunikaci mezi koncovými zařízeními a řídicím centrem na straně dodavatele energií. Díky této komunikaci má dodavatel okamžitý přehled o stavu sítě, zákazník (odběratel) má přístup k datům o spotřebě apod.



Obrázek 2: Smart Energy

Zdroj: [24]

1.2.3 Smart Environment

Smart Environment, neboli inteligentní prostředí, se podle Marka Weisera vyvíjí ze všudypřítomných výpočtů a podporuje myšlenky *„fyzického světa, který je bohatě a neviditelně protkán senzory, ovladači, displeji a jinými výpočetními prvky, které jsou bezproblémově zakotveny v předmětech každodenního života, a propojené prostřednictvím jedné sítě“*. [35]

Životní prostředí také hraje roli při vytváření chytrých měst. Tato část konceptu si klade za cíl snižování uhlíkové stopy, využívání čistých a obnovitelných zdrojů energie a nakládání s odpadem.

1.2.4 Smart Buildings

Budovy tvoří až 40 % světové spotřeby energie [18]. Chytré budovy jsou takové stavby, které používají automatizované procesy ke kontrole a správě celého objektu. Může se jednat o vytápění, ventilaci, osvětlení, zabezpečení a celou řadu dalších systémů. Jelikož provoz energeticky neefektivních budov se může prodražit, je vhodné uvažovat o použití chytrých technologií i zde. Modernizace infrastruktury staveb zaručuje nejen vyšší energetickou efektivitu a snížení emisí, ale také zvýšení bezpečnosti (např. ochrana před požárem). [33][17]

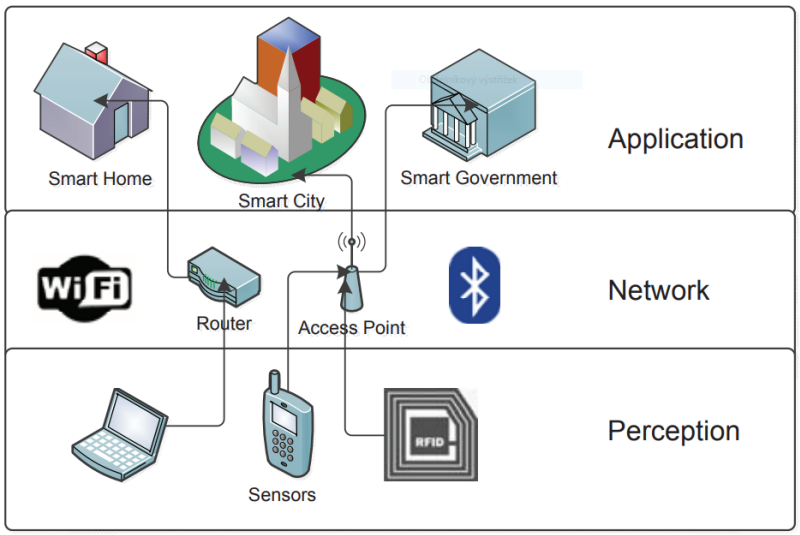
V roce 2016 byly v rámci Pardubického kraje provedeny energetické úspory u celkem 17 objektů s celkovou garantovanou úsporou 71 milionů korun během 10 let. Projekty, které byly v rámci Pardubického kraje zrealizovány, čítají dodání celkem 13 nových kotelen, instalaci tří kogeneračních jednotek, fotovoltaických panelů či výměnu téměř 2 900 svítidel. Dále byl instalován systém řízení odběru elektrické energie pro sedm objektů a zajištěno osazení více než 2 500 spořičů vody. [17]

Je důležité zdůraznit, že terminologie v oblasti konceptu inteligentních měst (Smart City) zatím není zcela ustálená, jelikož neexistuje všeobecně uznávaná definice. Samotný koncept je často vnímán a vykládán z různých úhlů pohledu.

1.3 Architektura IoT technologií

Koncept Smart City je jednou z mnoha aplikačních oblastí konceptu Internet of Things (Internet věcí). Ten se skládá ze senzorů a zařízení, které jsou začleněny do běžných objektů a připojeny k síti (po pevných linkách nebo bezdrátově). Tato kapitola popisuje architekturu zařízení Internetu věcí.

V IoT je každá vrstva definována svou funkcí a zařízeními, které jsou v dané vrstvě použity. Dle názoru odborníků IoT využívá převážně 3 vrstvy: perception layer, network layer, application layer. [22]



Obrázek 3: Vrstvy IoT

Zdroj: [22]

1.3.1 Perception layer – vrstva vnímání

Vrstva vnímání, v některých publikacích pod názvem senzorová, získává data z prostředí pomocí senzorů Tato vrstva detekuje a sbírá informace, a také zajišťuje spolupráci mezi uzly (node) IoT zařízení v lokálních sítích a sítích krátkého dosahu. V případech, kdy je potřeba rychlé rozhodnutí, mohou být data zpracována už na této úrovni, ačkoliv výpočetní výkon jednotlivých IoT zařízení bývá omezený. Pro hlubší zpracování, které vyžaduje náročnější výpočty, je nezbytné data přesunout do cloudových nebo datových center. Přesun dat mezi senzory a datovými centry je realizován na následující vrstvě. [22]

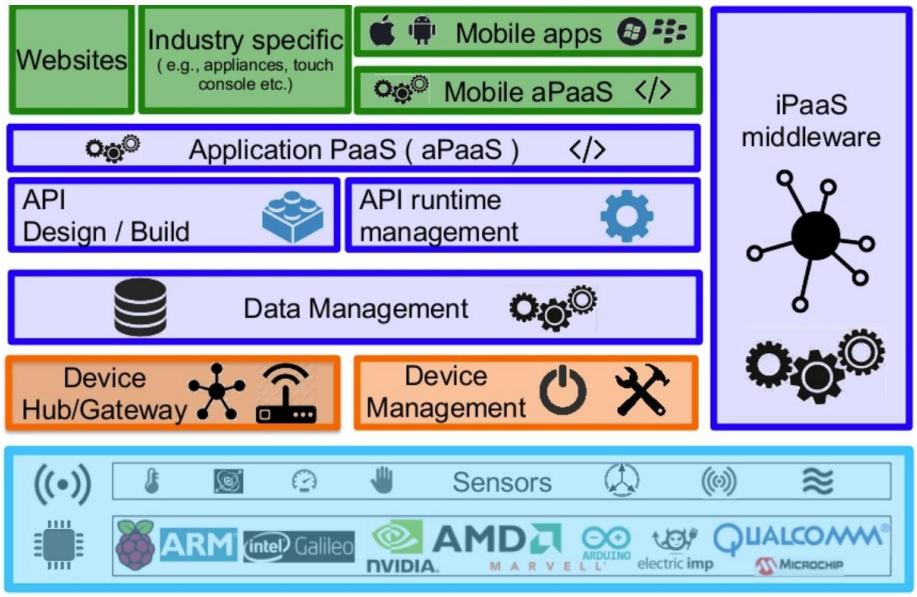
1.3.2 Network layer – síťová vrstva

Data ze síťové vrstvy jsou v analogové formě, a proto musí být digitalizována, aby bylo možné jejich následné zpracování. Síťová vrstva v IoT slouží k směrování a přenosu dat mezi rozbočovači a zařízeními přes Internet. Na této vrstvě fungují platformy cloud computingu[1], brány, routery a směrovače. Využívají některé z technologií jako jsou WiFi, LTE, Bluetooth, ZigBee apod. Síťové brány slouží jako prostředník mezi IoT uzly tím, že agregují, filtrují a přenáší data z a do různých senzorů. [22]

1.3.3 Application layer – aplikační vrstva

Aplikační vrstva zaručuje důvěrnost, integritu a autenticitu dat (CIA – Confidentiality, Integrity, Availability). Na této vrstvě jsou také dosaženy cíle konceptu IoT, čili vytvoření inteligentního prostředí.

Obrázek 4 zobrazuje architekturu IoT, světle modrá – senzorová vrstva, oranžová – síťová vrstva, modrá – aplikační vrstva, zelená – uživatelské rozhraní.



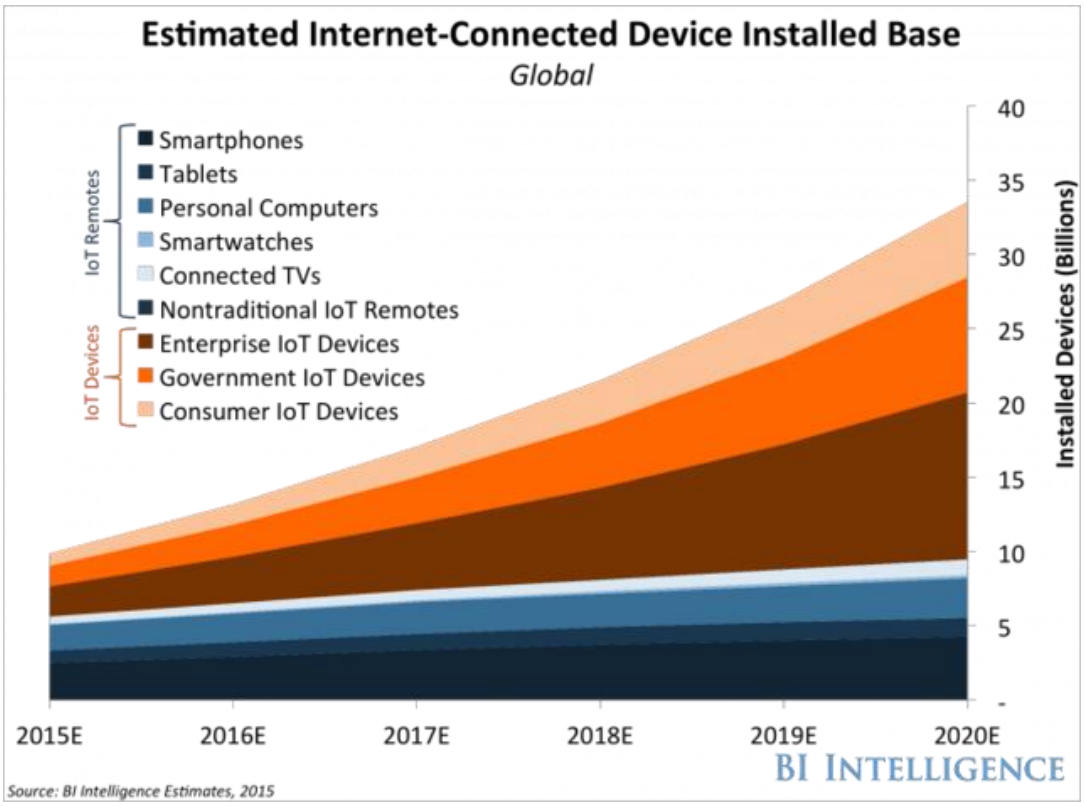
Obrázek 4: Architektura IoT

Zdroj: [30]

[1] Cloud computing lze charakterizovat jako poskytování služeb či programů servery dostupnými z Internetu s tím, že uživatelé k nim mohou přistupovat vzdáleně, např. pomocí webového prohlížeče.

1.4 Trendy v IoT

V současnosti se počet připojených IoT zařízení zvyšuje velmi rychle. Web Business Insider predikuje exponenciální nárůst. V předpovědi je uvedeno, že v roce 2020 bude připojeno přes 34 miliard IoT zařízení (jakékoliv zařízení, které je samostatně připojené k síti Internet a může být monitorováno a/nebo ovládáno vzdáleně). Roku 2015 bylo připojeno pouze 10 miliard zařízení. IoT zařízení tedy budou tvořit 70 % všech připojených zařízení, zbylých 30 % zastupuje tradiční výpočetní technika (např. smartphony, tablety atd.). V následujících letech také bude do IoT investováno téměř 6 bilionů (10^{12}) amerických dolarů (viz Obrázek 5). [8]



Obrázek 5: Předpověď trendů v IoT

Zdroj: [8]

2 IDENTIFIKACE ZRANITELNÝCH MÍST

Počet připojených IoT zařízení neustále zvyšuje. [8] V mnoha městech již je Internet věcí hojně využíván. Aby bylo možné město považovat za chytré, musí používat inteligentní technologie v oblastech kritické infrastruktury. Taková inovace poskytuje mnoho výhod, například nižší energetické náklady nebo vyšší bezpečnost dopravy, zároveň však jsou tyto systémy ohroženy hackerskými útoky. Vzhledem k tomu, že města jsou zodpovědná za 70 % spotřeby veškeré energie a generují 70 % světového hrubého domácího produktu (GDP)[18], jakýkoliv pokus o sabotáž může mít na chytrá města velký dopad. Rizika ignorování těchto bezpečnostních hrozeb jsou vysoká, zneužití byť jediného zařízení, může mít za výsledek ohrožení celého systému nebo sítě.

Mnoho chytrých zařízení má z důvodu potřeby nízké hmotnosti omezený výpočetní výkon – pouze ke splnění základních funkcí daného zařízení. Z toho důvodu je obtížné provádět šifrování dat. Dalším technologickým problémem je nedostupnost aktualizací softwaru. Systémy s původním firmwarem budou vždy náchylné ke zneužití. [33]

V této kapitole budou uvedena zranitelná místa, které může potenciální útočník zneužít a ohrozit tím celkové zabezpečení senzorů a přenosových cest.

2.1 Komunikační technologie

Technologie používané v chytrých městech jsou propojeny pomocí několika komunikačních technologií a protokolů jako jsou 4G LTE, GSM, CDMA, WiFi, Bluetooth, NFC a bezdrátový standard ZigBee. Všechny z uvedených jsou využívány k vytváření sítí a přenosu dat a také mají bezpečnostní mezery – přenášená data mohou být zachycena třetí stranou, která získá neoprávněný přístup. Některé z těchto protokolů jsou natolik komplikované, že je velmi obtížné je bezpečně a zároveň efektivně implementovat. [20]

2.2 Nevhodná implementace

Hlavní problém bezpečnostních rizik chytrého města spočívá v tom, jak jsou technologie implementovány v celém svém kontextu. Jak jsou systémy a zařízení nakonfigurovány ovlivňuje, zda jsou náchylné k útokům. Zařízení s otevřenými porty nebo továrně navrženými zadními vrátky (backdoor) lze snadno najít a zneužít. Mnoho zařízení, která jsou připojená do sítě Internet, má veřejně dostupný zdrojový kód a výchozí přihlašovací údaje, čehož může být také snadno využito k provedení útoku. [33]

Další problém představují softwarové chyby – bugy, které mohou mít dalekosáhlý dopad. Příkladem může být závada softwaru ke které došlo v listopadu 2013 v San Francisku. Systém veřejné dopravy Bay Area Rapid Transit (BART) byl vypnut kvůli technickým problémům zahrnujícím přepínání tratí, ohroženo bylo 19 vlaků s přibližně 500 až 1000 cestujícími. [11]

2.3 Motivace útočníka

Útočník si může zvolit za cíl prvky chytrého města z mnoha důvodů, například aby si vyzkoušel svoje schopnosti. Mnohem závažnější mohou být útoky kyber-zločinců, kteří zneužijí zařízení a systémy Smart City ke krádeži peněz nebo osobních dat uživatelů. V extrémních případech může být útok na infrastrukturu Smart City součástí teroristických činů nebo kybernetické války [33][8]. Ať už je motivace útočníka jakákoliv, obecně lze říci, že bude postupovat v následujících krocích (viz Obrázek 6):

Krok 1: Statická analýza

Za použití veřejně dostupného firmwaru, kódu a aplikací provede útočník statickou analýzu zařízení a systémů. Cílem je odhalit slabá místa, které mohou být následně zneužita.

Krok 2: Skenování

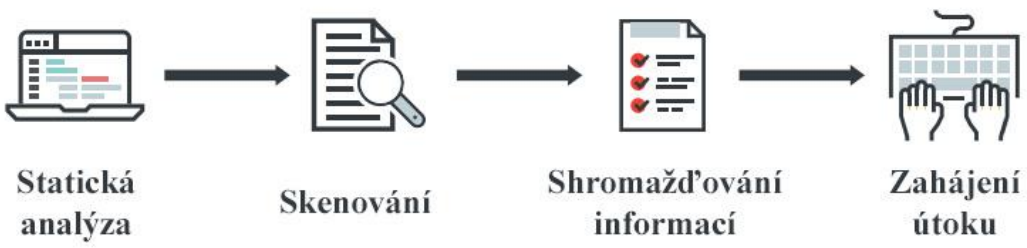
V dalším kroku útočník provede skenování zranitelných zařízení a systémů, aby určil svůj cíl a vstupní místa.

Krok 3: Shromažďování informací

Pomocí data miningu, phishingu nebo metod sociálního inženýrství získá relevantní informace (např. přihlašovací údaje).

Krok 4: Zahájení útoku

Jakmile útočník získá všechny potřebné části, může zahájit několik typů útoku. Například změnit zdrojový kód, infikovat systémy malwarem, poškodit zařízení (brick) atd.



Obrázek 6: Postup přípravy útoku

Zdroj: upraveno podle [33]

2.4 Možné způsoby útoků

Každá z vrstev IoT je náchylná k bezpečnostním rizikům a útokům. Ty je možné rozdělit na aktivní a pasivní. Pasivní útoky pouze monitorují informace bez narušení služeb (např. Spoofing nebo Man-in-the-middle útoky). Aktivní útoky přímo přerušují funkčnost služeb (např. ransomware[2]). Všechny vrstvy jsou náchylné k útokům typu DoS, které činí zařízení nebo síť nedostupnými pro oprávněné uživatele. [12][22]

2.4.1 Útoky na fyzickou vrstvu

Útoky na úrovni fyzické vrstvy OSI modelu vyžadují neoprávněný fyzický přístup k snímacím, ovládacím a řídicím systémům. Senzorové uzly IoT zařízení obvykle pracují ve venkovních prostorách, což může vést k fyzickým útokům, při nichž útočník manipuluje s hardwarem a komponenty zařízení. Z toho důvodu, pokud útočník získá fyzický přístup k zařízení, může způsobit významná poškození průmyslových zařízení a kritické infrastruktury. [5][22]

2.4.2 Útoky na přenosové vrstvy

Největší slabinou IoT zařízení je jejich síťová konektivita. Mechanismus výměny klíčů v IoT musí být dostatečně bezpečný, aby se zabránilo odposlechu a následné krádeži totožnosti. To je může učinit vzdáleně zneužitelnými. [5]

Zde existuje řada možných útoků přímo na zařízeních nebo uzlech (node), připojených k síti. Tyto uzly typicky komunikují s bránou (gateway), která je jádrem tohoto řešení. Uzel propojuje všechna připojená zařízení do sítě, případně cloudu. Jak již bylo zmíněno, síťová vrstva je náchylná k útokům typu DoS, zároveň může být napadena důvěrnost v síti prostřednictvím analýzy provozu, odposlechu a pasivního sledování (útok typu Man-in-the-middle). [22][23]

2.4.3 Útoky na aplikační vrstvy

Do této kategorie, kromě typických variant malwaru (viry, červy a trojské koně), patří také „fuzzing“, během kterého jsou programu poskytnuta náhodná, případně chybná data, což má za následek jeho zahlcení a zablokování [5]. Do této kategorie lze také zařadit botnet, což je síť počítačů, nebo zařízení napadených malwarem. Pokud má IoT zařízení přístup k Internetu,

2 Druh škodlivého programu, který blokuje počítačový systém nebo šifruje data v něm zapsaná, a poté požaduje od oběti výkupné za obnovení přístupu.

může se stát součástí botnetu. Příkladem je útok ze září 2016. Tehdy se útočníci pomocí botnetu Mirai pokusili zahltit server webu KrebsOnSecurity.com, podařilo se jim vygenerovat až 620 Gb/s. Vše nasvědčuje tomu, že k útoku bylo zneužito velké množství slabě – nebo vůbec – zabezpečených IoT zařízení, převážně IP kamer. [21]

2.4.4 Možné útoky v jednotlivých oblastech Smart City

V následující tabulce (Tabulka 1) jsou zobrazeny některé potenciální útoky na každý sektor Smart City.

Tabulka 1: Možné útoky na Smart City

	Ohrožení bezpečnosti	**Finance**	**Činnost**	**Soukromí**
Energetika	Způsobení nestabilních dodávek el. proudu	Ransomware útoky nebo krádež energie	Přerušení dodávek el. energie	Odposlech elektroměrů, krádež informací
Doprava	Způsobení dopravních nehod	Využití slabin k získání bezplatné jízdy	Přerušení a manipulace s dopravními prostředky	Ohrožení údajů o uživatelích
Prostředí		Držení systémů a zařízení jako rukojmí (ransomware)	Přerušení reakcí systému	Využití senzorů ke sledování aktivity
Připojení		Držení systémů a zařízení jako rukojmí (ransomware)	Přerušení síťové komunikace (DoS)	Odposlech a krádež údajů
Veřejná správa		Držení systémů a zařízení jako rukojmí (ransomware)	DoS Přeměna zařízení na boty (botnet)	Shromažďování informací skrze monitorovací zdroje a open data

Zdroj: upraveno podle [33]

2.5 Rizika technologií IoT

Následující tabulka (Tabulka 2) přehledně zobrazuje zranitelná místa v jednotlivých částech zařízení Internetu věcí (IoT).

Tabulka 2: Oblasti a zranitelnost prvků IoT

Oblast útoku	Zranitelnost
Paměť zařízení	Cleartextová uživatelská jména Cleartextová hesla Pověření třetích stran Šifrovací klíče
Fyzické rozhraní zařízení	Extrakce firmwaru Rozhraní příkazového řádku Reset do nezabezpečeného stavu Odstranění paměťových médií
Webové rozhraní zařízení	SQL injection Slabá hesla Zablokování účtu Známé výchozí přihlašovací údaje
Firmware zařízení	Nešifrované přihlašovací údaje Zobrazení verze/poslední aktualizace firmwaru Odhalení citlivých adres URL Šifrovací klíče
Síťové služby zařízení	Rozhraní příkazového řádku Injection Denial of Service Nešifrované služby Přetečení na zásobníku (buffer overflow) [13] Zranitelné služby UDP Universal Plug and Play

Oblast útoku	Zranitelnost
Místní úložiště dat	Nešifrovaná data Data šifrovaná objevenými klíči Nedostatečná kontrola integrity dat
Backend API	Slabá autentizace Slabá kontrola přístupu Injekční útoky Prozrazení informací
Webové rozhraní cloudu	SQL injection Slabá hesla Zablokování účtu Známé výchozí přihlašovací údaje Šifrování přenosu Nezabezpečený mechanismus obnovení hesla
Aktualizace	Odeslaná nešifrovaná aktualizace Nepodepsaná aktualizace Ověření aktualizace Škodlivá aktualizace Chybějící možnost aktualizace
Administrativní rozhraní	SQL injection Slabá hesla Zablokování účtu Známé výchozí přihlašovací údaje Nemožnost vymazat zařízení Možnosti logování

Zdroj: upraveno podle [19]

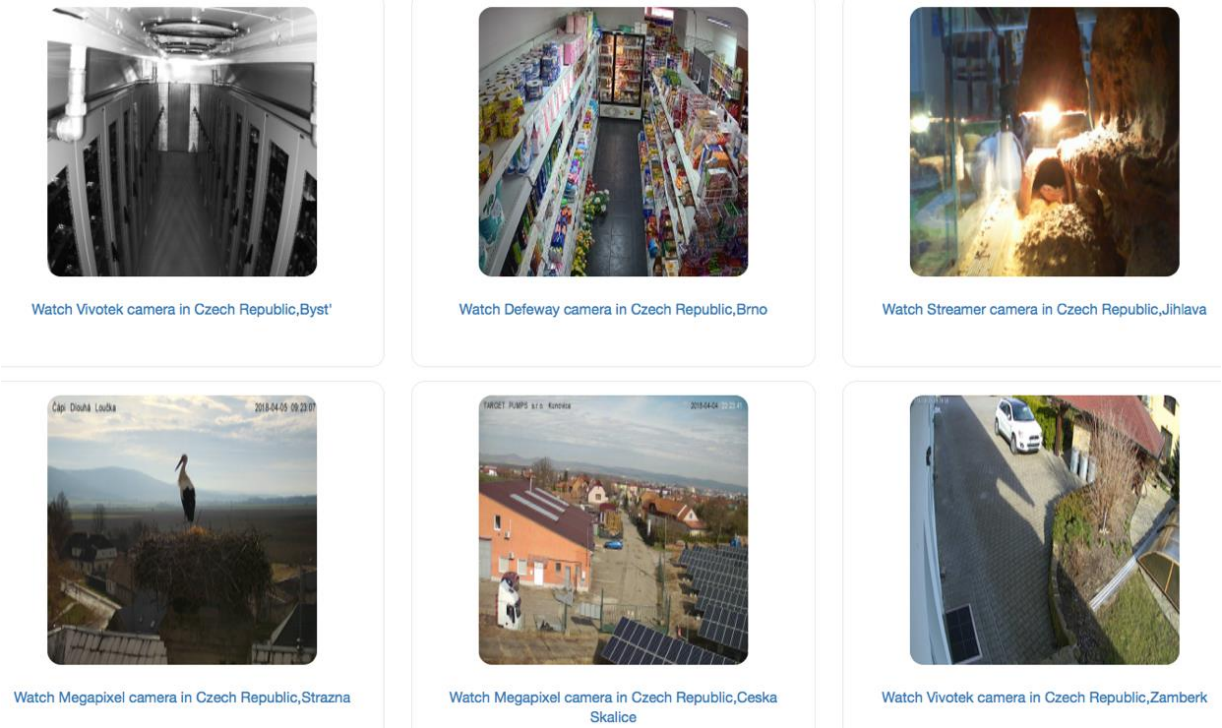
2.6 Zdokumentované útoky

V této podkapitole bude uvedeno několik zdokumentovaných útoků a s nimi souvisejících bezpečnostních hrozeb. Jedná se pouze o zlomek útoků, sloužících k demonstraci zranitelnosti technologií Smart City.

V roce 2016 prohlásil manažer informační bezpečnosti pro San Diego, USA, že jejich systémy jsou zasaženy průměrně 60 000 kyber-útoky denně [3]. Ve studii z roku 2014, kterou provedlo téměř 600 energetických, těžařských a výrobních společností, kolem 70 % nahlásilo nejméně jeden bezpečnostní incident, který vedl ke ztrátě důvěrných informací nebo přerušení operací v následujícím roce. [27]

Mimo útoků na energetickou síť je také registrováno mnoho případů, kdy cílem byla doprava. Ve Spojených státech Amerických byly napadeny systémy řízení letového provozu, kompromitovány servery FAA, nainstalován škodlivý kód do kontrolních sítí a ukradeno 58 tisíc osobních údajů zaměstnanců [15]. Dalším případem je útok teenagera v polské Lodži, kterému se podařilo nabourat do systému výhybek, čímž způsobil vykolejení čtyř tramvají a zranění několika cestujících [26].

Pro další demonstraci zranitelnosti IoT slouží web Insecam.org (Obrázek 7), který poskytuje přístup k tisícovkám nezabezpečených IP kamer z různých částí světa, včetně České republiky.



Obrázek 7: Nezabezpečené IP kamery

Zdroj: vlastní zpracování podle www.insecam.org

3 NÁVRH ZABEZPEČENÍ SENZOROVÝCH PROSTŘEDKŮ

V této kapitole bude uvedena případová studie s fiktivním městem v České republice, pro kterou bude navrženo několik možných využití moderních technologií, které mají za cíl zlepšit kvalitu života a efektivitu každodenních činností. Následně bude navrženo zabezpečení senzorů a přenosových cest vybraných prvků.

Jelikož koncept Smart City zatím není v České republice příliš rozšířený, bude využito již existujících řešení ze zahraničí a některé vhodné prvky použity u návrhu fiktivního chytrého města v ČR. Lze předpokládat, že návrhem pro velká, např. krajská města, se budou zabývat komerční společnosti poskytující komplexní řešení „na míru“. Vzhledem ke komplikovanosti návrhu je tato práce zaměřena na středně velká města. Některé prvky je poté možné dle návrhu aplikovat i u měst s menší rozlohou a počtem obyvatel.

Pro demonstraci bude vytvořeno fiktivní město, které bude pro potřeby této práce charakterizováno několika geografickými, politickými, ekonomickými a sociodemografickými vlastnostmi.

Při návrhu inteligentního města budou využity již získané znalosti a zkušenosti z metodiky Ministerstva pro místní rozvoj ČR. [14]

3.1 Výchozí situace

Pro potřeby této práce není důležité použití reálné předlohy, proto bude nevrženo obecné Město M, které poskytne co nejširší možnosti pro využití komponent Smart City a řešení problémů běžného života ve městech. Předlohou pro fiktivní Město M použité v této práci je několik okresních měst v České republice.

Město M

Město M je v postavení obce s rozšířenou působností a má přibližně 40 tisíc obyvatel.

Členění města:

Město má historické jádro s náměstím a kostelem. Zároveň je v okolí několik pamětihodností a historických budov, vč. městské radnice. Také městem protéká řeka. Na periferii se vyskytuje moderní zástavba obytných a rodinných domů.

Vzdělávání:

Ve městě je několik mateřských a základních škol, dále střední odborné učiliště a gymnázium.

Doprava:

Městem prochází silnice první třídy, která spojuje okolní města a představuje významnou tranzitní trasu v kraji. Ve městě jsou čtyři křižovatky se světelným signalizačním zařízením (tzv. semafor). Ve městě je autobusové a železniční nádraží. Zároveň město na svém území provozuje městskou hromadnou dopravu.

Občanská vybavenost:

Kromě drobných maloobchodů je ve městě také obchodní centrum s parkovištěm. V okrajové části se vyskytuje průmyslová zóna, ve které je několik výrobních firem. Ve městě je také nemocnice, stanice hasičského záchranného sboru a obecní policie.

3.2 Návrh použití senzorových prostředků

V této kapitole bude uvedeno několik možných řešení pro jednotlivé oblasti chytrého města, samotné zabezpečení bude specifikováno v kapitole 3.3.

3.2.1 Doprava

Vylepšení mobility a snížení dopravního zatížení jsou jen některé z výzev, kterým čelí dnešní města. Dopravní zácpy ovlivňují každodenní život dojíždějících obyvatel a návštěvníků města. Z toho důvodu hledá mnoho měst inteligentní dopravní řešení, která minimalizují dopravní zácpy a optimalizují využití městské hromadné dopravy.

3.2.1.1 Veřejná doprava

Vzhledem k tomu, že ve městě je autobusové a železniční nádraží a MHD, je vhodné uvažovat o použití inteligentních dopravních systémů (ITS). Mezi hlavní pilíře ITS patří správa veřejné dopravy, informace o trase, elektronický rozvrh a platební systém.

Automatický systém pro určení polohy vozidla (AVLS) kombinuje technologie GPS a GPRS k odeslání polohy vozidla do řídicího centra. V návaznosti pracují informační systémy pro cestující (PIS), které poskytují dynamické informace o spojích v reálném čase.

Inteligentní řešení pro vlaky a autobusy nabízí firma Cisco. Pomocí IP protokolu jsou vozidla schopna přenášet data z jedné sítě do dalších během pohybu v tranzitním nebo železničním systému. Tato data jsou poté zpracována a využita v PIS. [9]

3.2.1.2 Parkoviště

Mezi hlavní výhody „chytrého parkování“ patří efektivnější vedení dopravy, dodržování emisních předpisů, zvýšení příjmů (za parkovací poplatky) a možnosti predikce a práce s daty v reálném čase. Pro samotné řidiče to poté znamená komfortnější dopravu, ušetřené náklady a jednodušší parkování.

Zajímavé řešení parkování automobilů ve městě nabízí společnost Siemens – Intelligent City Parking. Tato technologie používá pro detekci radar bez kamery (Obrázek 8), který může být instalován například na sloupech veřejného osvětlení nebo zdech budov. Senzory vysílají mikrovlny do předem stanoveného prostoru, pokud narazí na překážku, odrazí se zpět k senzoru a ten je zachytí. Jsou schopné pracovat v různých světelných a klimatických podmínkách, a zároveň nepoužívají fotoaparát, čímž nejsou porušovány práva na ochranu osobních údajů občanů. Tento radar může pracovat autonomně nebo v kombinaci s parkovacími automaty. [17]

Dalším prvkem bude použití parkovacích automatů s platebním terminálem, které umožnují platbu parkovacího poplatku v hotovosti případně platební kartou.

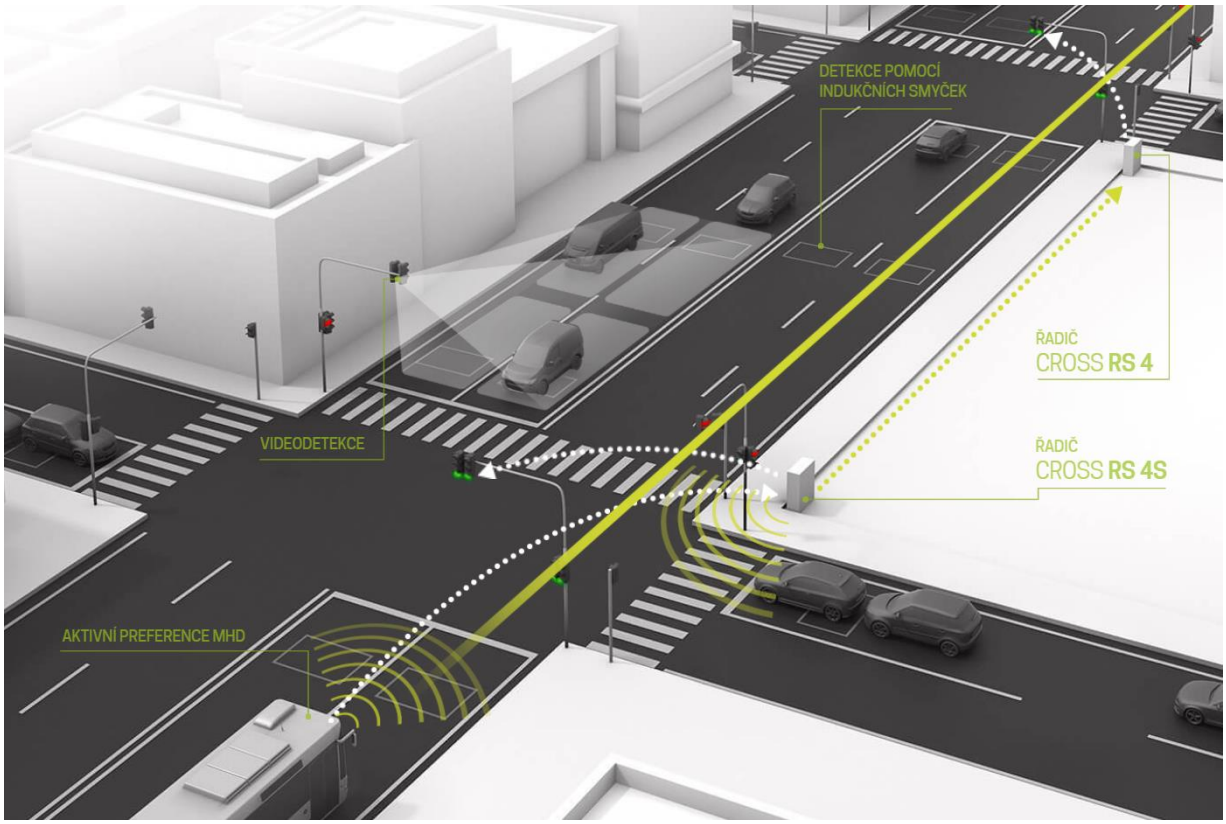
Obrázek 8: Radar na sloupu veřejného osvětlení

Zdroj: [17]

3.2.1.3 Světelné signalizační zařízení

Jak již bylo uvedeno, ve městě jsou čtyři křižovatky se světelným signalizačním zařízením. Vhodným nastavením těchto zařízení je možné regulovat provoz ve městě a reagovat na neobvyklé situace, např. průjezd vozidel s právem přednostní jízdy.

Systémy řízení dopravy se zabývá česká firma CROSS Zlín a.s., jejich řešení využívá řadiče SSZ, detekci pomocí indukčních smyček a video detekci k optimalizaci řízení dopravy v městských oblastech (viz Obrázek 9). Zároveň umožňuje aktivní preferenci vozidel MHD a vyvolání tras pro průjezd vozidel IZS. Řadiče mohou pracovat decentralizovaně nebo s připojením na dopravně-řídicí centrálu. Tento systém je nyní provozován ve Zlíně, kde zrychlil průjezd vozidel MHD až o 20 %. [17]



Obrázek 9: Systém řízení dopravy

Zdroj: [28]

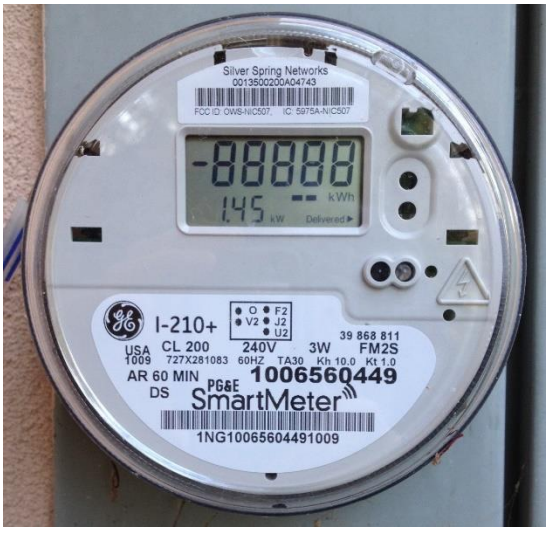
3.2.2 Energetika

Dalším velmi důležitým pilířem Smart City je energetika, vytvoření inteligentních sítí je jedním z mnoha cílů. Mezi další patří snižování emisí oxidu uhličitého (CO_2), skladování, distribuce a výroba elektrické energie, využívání čistých a udržitelných energetických zdrojů atp. K zajištění čisté a obnovitelné energie mohou být využity solární a větrné elektrárny a vodík.

3.2.2.1 SmartMeter

Chytré měřiče (el. energie a/nebo plynu) zaznamenávají spotřebu energie v přednastavených intervalech (obvykle každých 15 nebo 30 minut) a odesílají nashromážděná data poskytovateli služeb. Měřiče používají systémy automatického čtení (AMR), které používají rádiové vysílače, mobilní připojení nebo antény na střechách, které prostřednictvím Wi-Fi, ISM rádiového pásma nebo mobilní sítě odesílá data do sítě [33]. Nespornou výhodou je, že domácnosti se nebudou spoléhat na odhadované faktury za energii ani poskytovat vlastní pravidelné údaje (odečet elektroměru). Instalaci SmartMeteru (viz Obrázek 10) by měl zpravidla provádět dodavatel energie.

Pro účely testování a pilotního provozu osadila společnost ČEZ v roce 2011 celkem 40 tisíc domácností inteligentními měřidly – v tendru zvítězilo konsorcium Hawlett Packard [32].



Obrázek 10: SmartMeter

Zdroj: [20]

3.2.2.2 Veřejné osvětlení

Inteligentní veřejné osvětlení pomáhá městům šetřit spotřebu energie a snižovat náklady náhradou konvenčních zdrojů světla (sodíkových a halogenidových) za LED. Dalším efektem je snížení emisí CO_2 a světelného smogu, při současném zlepšení poskytovaných služeb. Veřejné osvětlení má vliv na bezpečnost a viditelnost na vozovkách. Při komplexním řešení Smart City je možné sloupy veřejného osvětlení využít také pro instalaci dalších senzorů, např. sledování kvality ovzduší nebo hluku. Zároveň je při návrhu a implementaci nutné dodržet normové hodnoty dle ČSN EN 13201 - Osvětlení pozemních komunikací.

Stávající běžné řešení veřejného osvětlení je velmi neefektivní, každá lampa pracuje nezávisle a svítí plnou intenzitou obvykle 10-12 hodin denně. Pro inteligentní osvětlení existují tři moderní přístupy. První přístup pracuje se zpožděním, lampa svítí plnou intenzitou, pokud pohybový senzor detekuje něčí přítomnost v jejím dosahu, pakliže v dosahu není žádný chodec a uplyne určitý časový interval, lampa svítit přestane. Druhý přístup je modifikací prvního, lampa se zapne pouze v případě, že senzor zachytí v blízkosti chodce a poté lampa svítí až do konce přednastaveného intervalu (do rána). Třetí přístup – ztlumení, svítivost je upravena podle počtu uživatelů v okolí, čím větší je počet chodců v okolí lampy, tím silnější světelná intenzita. [19] Všechny přístupy zobrazuje Tabulka 3.

Tabulka 3: Přístupy k inteligentnímu osvětlení

Metoda	Popis	Efektivita
Běžná	Lampa je aktivní celý interval a svítí maximální intenzitou.	Nízká
Zpoždění	Lampa se zapne v případě, že uživatel je v její blízkosti. Pokud v jejím dosahu nikdo není, je aktivní po určitý časový úsek a poté se vypne.	Vysoká
Setkání	Lampa se zapne při prvním setkání s alespoň jedním uživatelem a poté je aktivní po celý zbytek noci.	Střední
Ztlumení	Lampa svítí 60 % intenzitou, pokud v okolí nikdo není. Automaticky zvyšuje/snižuje intenzitu podle počtu chodců v okolí.	Vysoká

Zdroj: upraveno podle:[19]

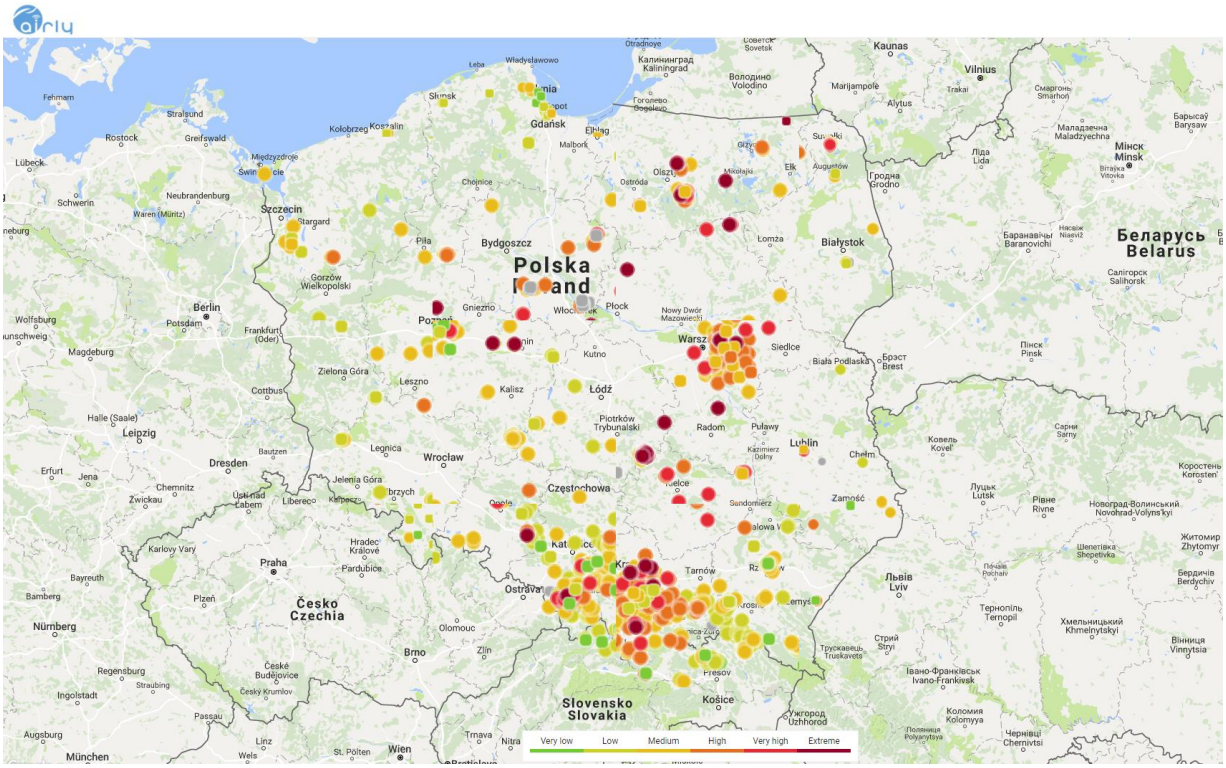
Z analýzy je patrné, že největší efektivity dosáhneme při použití LED osvětlení a metody ztlumení. Návratnost nákladů na výměnu existujících sodíkových výbojek za LED je mezi jedním a dvěma roky. [19]

3.2.3 Smart Environment

Kromě dopravy a energetiky hraje důležitou roli také samotné prostředí měst. Sledování kvality vzduchu umožňuje občanům rozhodnout, zda je vhodné trávit čas venku (pokud ovzduší není příliš znečištěné). Inteligentní systémy pro nakládání s pevnými odpady pak pomáhají řešit problémy s komunálním odpadem ve městech, skládkami a recyklací.

3.2.3.1 Systémy pro sledování kvality ovzduší

U projektů sledujících kvalitu ovzduší je kladen důraz na vysokou přesnost a konektivitu (dostupnost) a zároveň nízkou cenu. Takové senzory nabízí polská firma Airly, jejich síť snímačů je možné instalovat po celém městě nebo kraji a technologie umožňuje sledovat kvalitu ovzduší v reálném čase pomocí online mapy nebo mobilních aplikací. [22]



Obrázek 11: Mapa znečištění ovzduší

Zdroj: [1]

3.2.3.2 Systémy pro svoz odpadu

Popelářské vozy běžně jezdí pravidelně po pevně daných trasách. Sváženy jsou prázdné i plné kontejnery komunálního odpadu. Tento postup lze zefektivnit použitím vhodných algoritmů a zavedením dynamického systému, který snižuje náklady tím, že optimalizuje trasu a zvyšuje účinnost svozu. Za zmínku stojí pneumatický odpadový systém odsávající odpad na centrální místo, který používá město Songdo IBD v Jižní Koreji [14]. Většina měst, obzvlášť pokud mají historické jádro, takový systém použít nemůže, a proto využijí inteligentní kontejnery se senzory.

Například Filadelfie, Hamburg, Melbourne a další světová města používají solárně napájené chytré kontejnery Bigbelly. Součástí kontejneru je solární panel, který dobíjí vnitřní baterii, LED indikátory a používá GPRS pro online monitorování a management. Když množství odpadu dosáhne určité úrovně (měřeno pomocí tlakového senzoru), je obsah stlačen pomocí lisu. V případě úplného zaplnění nádoby je tato informace ihned pomocí bezdrátových technologií odeslána do cloudového systému CLEAN, který sleduje všechny stanice v dané oblasti a nabízí jejich kompletní správu a přehled s možností plánování trasy svozu. [24]

Tyto chytré popelnice začala již v některých městských částech používat Praha. První čísla ukazují, že ve zkušebním provozu se podle oficiálních údajů optimalizovala četnost svozu odpadů o 90 procent. Počet svozů klesl a náklady na svoz spadly až o 75 procent. Tam, kde dříve svozová auta jezdila až několikrát denně, nyní mohou dojet jednou týdně. [29]

Obrázek 12: Odpadkové koše Bigbelly v Praze

Zdroj: [29]

3.2.3.3 Veřejné bezpečnostní kamerové systémy

Jelikož je ve městě několik stanic IZS, má smysl uvažovat také o využití kamerového systému (CCTV). Účelem kamerových systémů je primárně zajištění bezpečnosti občanů, monitorování dopravní situace a v neposlední řadě boj proti zločinu. Jak již bylo zmíněno v kapitole 2.6, zabezpečení IP kamer je obecně na velmi nízké úrovni. Největší bezpečnostní riziko hrozí při napadení bezpečnostních kamer, které používá státní správa a integrovaný záchranný systém, zejména policisté a strážníci.

Z hlediska návrhu a implementace systémů CCTV je třeba brát v úvahu platnou legislativu, zejména zákon č. 101/2000 Sb. – zákon o ochraně osobních údajů a o změně některých zákonů. a také dodržení normy ČSN EN 50 132, především její sedmé části – pokyny pro aplikaci.

Při výběru technologií je možné volit z obrovského množství hardwaru, pokud splňuje několik základních specifikací, mezi které patří dostatečná rozlišovací schopnost kamer, možnost připojení do sítě a případně systém identifikace lidských tváří (Facial Recognition System). Další vlastnost, kterou je při výběru vhodné vzít v úvahu, je možnost souběžného využití kamer pro účely chytrého parkování (kapitola 3.2.1.2).

V návrhu bude použit kamerový systém složený z venkovních síťových kamer, které je možné instalovat prakticky kdekoliv – např. na sloupy veřejného osvětlení nebo zdi budov. Tyto kamery je proto vhodné umístit na nejfrekventovanější a nejrizikovější místa jako je náměstí, obchodní centrum, parkoviště a důležité dopravní uzly a křižovatky.

3.2.3.4 Veřejné Wi-Fi připojení

Inteligentní městská infrastruktura se opírá o spolehlivou a stabilní konektivitu. Veřejné Wi-Fi sítě jsou součástí širokopásmové infrastruktury poskytované obcemi a městy, která má za cíl zajištění pohodlného připojení pro obyvatele a návštěvníky a zajištění provozu městských služeb založených na IoT.

Navzdory jednoduchosti mohou být veřejné sítě pomalé a nestabilní, komunikační vzdálenost je v městských oblastech značně omezená. Přestože je možné využít běžné routery pro vytvoření hotspotu, v návrhu bude použit hardware speciálně vyvinutý pro poskytování veřejných Wi-Fi hotspotů.

Vhodnou kombinací s dalšími kompatibilními prvky Smart City, např. chytré odpadkové koše, lavičky nebo sloupy veřejného osvětlení, které mohou zároveň poskytovat veřejné Wi-Fi připojení, lze docílit velmi dobrého pokrytí napříč celým městem.

3.3 Zabezpečení senzorových prostředků

Tato kapitola se věnuje možnostem zabezpečení prostředků, zvolených v předchozí kapitole, a přenosových cest k získávání dat pro chytrá města.

3.3.1 Doprava

V této podkapitole jsou navrženy a popsány způsoby zabezpečení vybraných prvků z oblasti dopravní infrastruktury.

3.3.1.1 Veřejná doprava

Systémy pro správu veřejných dopravních prostředků mohou pro svou činnost využívat modul umístěný přímo ve vozidle (autobus, vlak apod.), který sbírá informace o aktuální poloze vozidla pomocí GPS a tato data odesílá do serveru dopravního podniku. Server poté přijaté informace zpracuje a zobrazí aktuální časy příjezdu na informační tabule. Pro účely tohoto návrhu předpokládejme, že samotný server je dostatečně zabezpečený (zabezpečení serveru není předmětem této práce).

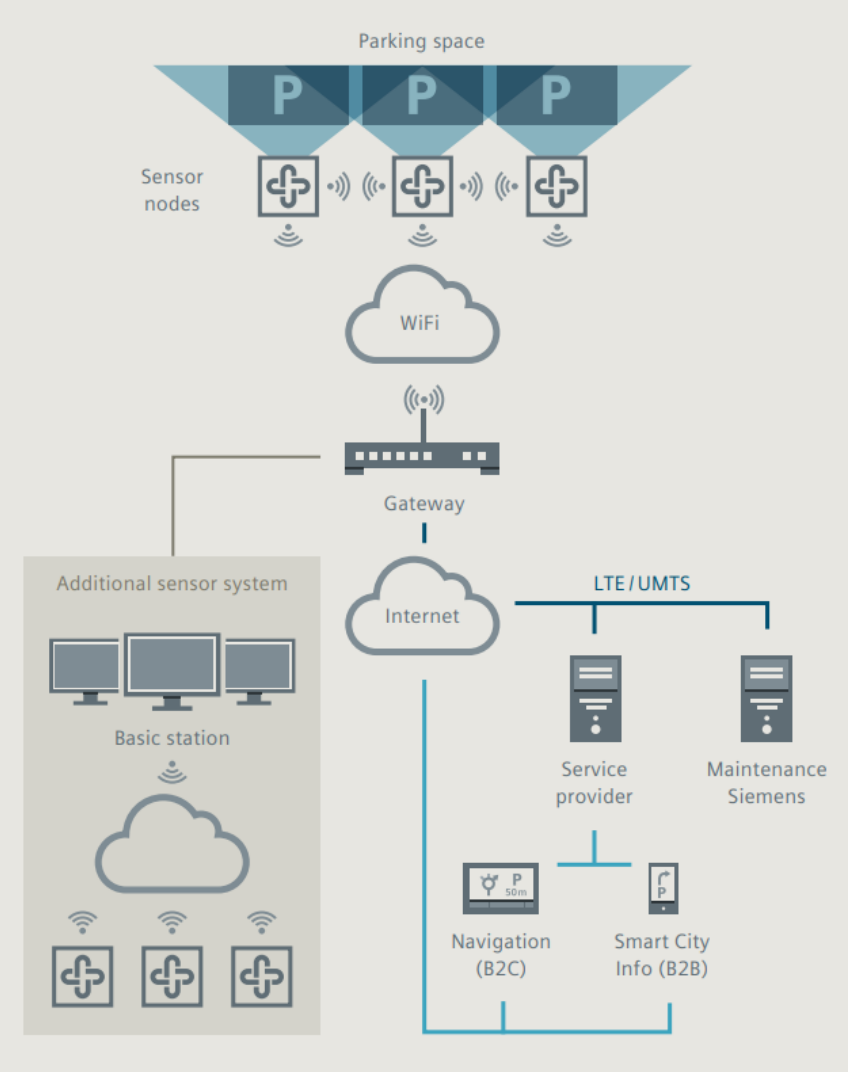
Modul ve vozidle se skládá z GSM/GPRS modemu, digitálního rychloměru, hodin reálného času a GPS přijímače. GPS přijímače pracují pasivně, slouží pouze pro příjem signálů z družic GPS, a tudíž není nutné jakkoliv je zabezpečovat. Přenos dat mezi vozidlem a serverem je realizován pomocí GSM/GPRS sítě. Standard GPRS, přestože je prováděno šifrování (pomocí proudové šifry A5/1), neposkytuje dostatečnou ochranu přenášených dat. Z toho důvodu je vhodnější použít standard 4G LTE, který k zabezpečení používá kryptografii symetrického klíče k ověření odesílatele a bezdrátově přenášená data šifruje.

3.3.1.2 Parkoviště

Systémy, které se zabývají parkováním vozidel ve městech, se mohou skládat z kombinace několika technologií. V tomto návrhu je použit běžný systém parkovacích automatů a současně senzory detekující přítomnost vozidel.

Jelikož parkovací automaty umožňují také platbu v hotovosti, musí být zabezpečeny proti krádeži. Toho lze docílit použitím pevných materiálů k výrobě pláště automatu, například ušlechtilé oceli. Tím bude zajištěna ochrana před vandalismem a okolními vlivy prostředí. Platební automaty mohou být bezdrátově připojeny k síti pomocí Wi-Fi.

Síť senzorů, které detekují přítomnost vozidel na parkovacích místech, je připojena pomocí Wi-Fi k bráně, která získaná data přenáší prostřednictvím Internetu do řídicího centra. Ke stejné bráně mohou být připojeny i platební terminály a automaty. Obrázek 13 zobrazuje celý systém chytrého parkování. Zabezpečením Wi-Fi spojení se zabývá kapitola 3.3.3.4 .



Obrázek 13: Chytré parkování

Zdroj: [31]

Některá řešení od jiných dodavatelů mohou pro připojení senzorů a monitorování parkovišť používat LPWAN, zabezpečení tohoto protokolu je popsáno v následujících kapitolách společně s dalšími senzory.

3.3.1.3 Světelné signalizační zařízení

Bezpečnostní expert společnosti IOActive Cesar Cerrudo, provedl v roce 2014 studii zabezpečení semaforů v USA, Austrálii, Kanadě a Francii: *"The vulnerabilities I found allow anyone to take complete control of the devices and send fake data to traffic control systems. Basically anyone could cause a traffic mess by launching an attack with a simple exploit programmed on cheap hardware ($100 or less)."* vysvětluje Cerrudo na svém blogu. [9]

Řadiče pro řízení silniční dopravy pomocí světelného signalizačního zařízení musí být v první řadě důkladně zajištěny proti neoprávněnému fyzickému přístupu, avšak zachována možnost přístupu pro oprávněné uživatele (např. Policie ČR). Toho lze docílit např. instalací řadiče do uzamykatelné schránky v blízkosti SSZ.

Pro spojení řadičů s dopravně řídicí centrálou lze využít optických vláken, která poskytují relativně vysokou bezpečnost přenosu a odolnost vůči elektromagnetické interferenci. Další možností je bezdrátové připojení přes radiový signál, které však může být nebezpečné zejména při použití nešifrovaných protokolů. V případě SSZ jsou nejčastěji používané bezdrátové vysílače pracující ve frekvencích 900MHz a 5,8GHz. Právě 5,8GHz verze je podobná protokolu 802.11n a vysílá SSID, které je viditelné z běžných mobilních zařízení, ale nelze se k němu připojit. Bezdrátová spojení nejsou šifrovaná a vysílače často používají tovární přihlašovací jména a hesla.

Pro bezpečnou implementaci takového řešení je proto nutné ovládací prvky a řadič zajistit proti neoprávněnému fyzickému přístupu a v případě bezdrátových spojení použít šifrování a vyvarovat se používání přednastavených přihlašovacích údajů. Řešení uvedené v kapitole 3.2.1.3 splňuje požadavky norem ČSN EN 50556 a ČSN EN 12675.

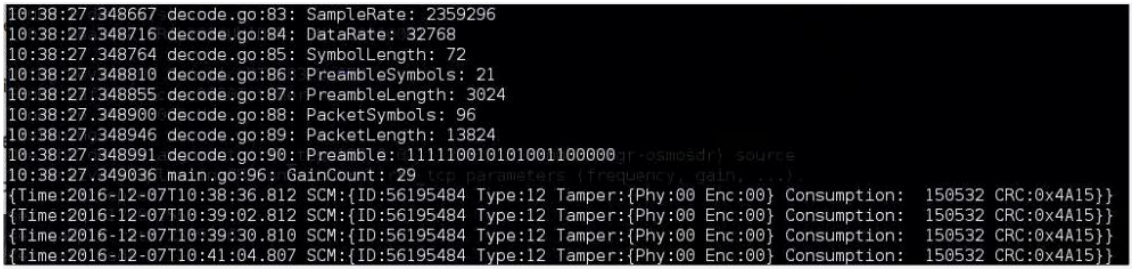
3.3.2 Energetika

V této podkapitole jsou navrženy a popsány způsoby zabezpečení vybraných prvků z oblasti energetiky.

3.3.2.1 SmartMeter

Používání chytrých měřičů představuje poměrně velkou hrozbu pro soukromí uživatelů. Podle spotřeby energie je možné odběratele profilovat a data zneužít k obchodním účelům. Měřiče pracující ve frekvenčním pásmu ISM a využívající Electronic Reporting Tool, mohou

být napadeny hackerským útokem a odposlouchávány, čímž útočník získá veškerá data. Pomocí levných USB zařízení lze poté data z chytrých měřičů číst (Obrázek 14).



Obrázek 14: Data z chytrého měřiče

Zdroj: [33]

Použití těchto měřidel je plně v kompetenci dodavatele energií, v tomto ohledu mohou města sehrát roli koordinační a částečně jako garanti bezpečnosti v případě vodovodní sítě.

S používáním chytrých měřičů také souvisí problematika Smart Grids, neboli chytré energetické sítě. Nasazením digitálních komponent do sítě dochází k digitalizaci dat a obousměrné komunikaci mezi správcem sítě a koncovými stanicemi. Jelikož se jedná o kritickou infrastrukturu, je nezbytné identifikovat všechna rizika a celou síť důsledně zabezpečit proti zneužití.

3.3.2.2 Veřejné osvětlení

V případě, že veřejné osvětlení není připojeno bezdrátově – ve většině případů to není nutné, je potřeba sloupy veřejného osvětlení zabezpečit proti fyzickému narušení a vandalismu. Řešení tohoto problému se nijak neliší od již stávajícího zabezpečení sloupů veřejného osvětlení.

Samotné sloupy jsou připojeny k elektrické síti, které poskytuje elektrickou energii pro jejich chod. Zároveň mohou světla distribuční síť využívat pro širokopásmové připojení pomocí EOP. Tento typ připojení využívá signály vyšší frekvence pro přenos internetových dat. Elektronické filtry na vstupu od sebe oba signály oddělí (Na podobném principu funguje připojení využívající telefonní linky – DSL). Takové připojení je obtížně napadnutelné a také poskytuje možnost ovládání sloupů veřejného osvětlení vzdáleně.

3.3.3 Smart Environment

V této podkapitole jsou navrženy a popsány způsoby zabezpečení vybraných prvků z oblasti Smart Environment.

3.3.3.1 Systémy pro sledování kvality ovzduší

Většina zařízení používá Linuxové kontrolery, které se spoléhají na běžné bezdrátové technologie jako Bluetooth nebo Wi-Fi. Vzhledem k nízkému výpočetnímu výkonu kontrolerů, jsou možnosti šifrování omezené. Přihlašovací údaje pro Wi-Fi připojení mohou být uloženy ve formě čistého textu v EEPROM paměti, zatímco Bluetooth připojení velmi často používá výchozí PIN 1234.

Senzory Airly použité v tomto návrhu využívají protokol LoRa[3] (Long Range) LPWAN, čili systémy, které je možné instalovat na velké rozloze (ve městech) a očekává se od nich velmi nízká spotřeba. Senzory, které jsou rozptýleny po celé oblasti, odesílají na server několik bajtů za hodinu. Používají frekvence 868MHz v evropském a 913MHz v americkém pásmu. Připojení jednotlivých uzlů (senzorů) je realizováno pomocí LoRa modulů a brány. Hardware LoRa modulů je obvykle založený na Arduino Uno, a slouží jako komunikační rozhraní. Externí brána je s jednotlivými uzly je brána připojena pomocí protokolu LoRaWAN a získaná data předává do cloudu.

Protokol LoRaWAN zajišťuje zabezpečený transparentní přenos dat z koncového zařízení a aplikací běžící na serveru. Šifrování zpráv je prováděno pomocí algoritmu AES128. Brána by také měla být zabezpečena proti fyzickému přístupu, jelikož jsou v ní uloženy informace jako například konfigurace a přihlašovací údaje ke cloudovému úložišti.

3 LoRa umožnuje přenos dat na velké vzdálenosti (více než 10 km v obydlených oblastech) s nízkými energetickými nároky. [25]

3.3.3.2 Systémy pro svoz odpadu

Řešení společnosti Bigbelly využívá ke svému fungování solárně napájené koše v kombinaci s cloudovou aplikací CLEAN – ta poskytuje dispečink přes webové rozhraní, plánuje a analyzuje svoz odpadových nádob Bigbelly. Jednotlivé nádoby jsou připojeny bezdrátově pomocí SIM karty přes GPRS nebo CDMA. Součástí nádob je i GPS modul pro určení polohy.

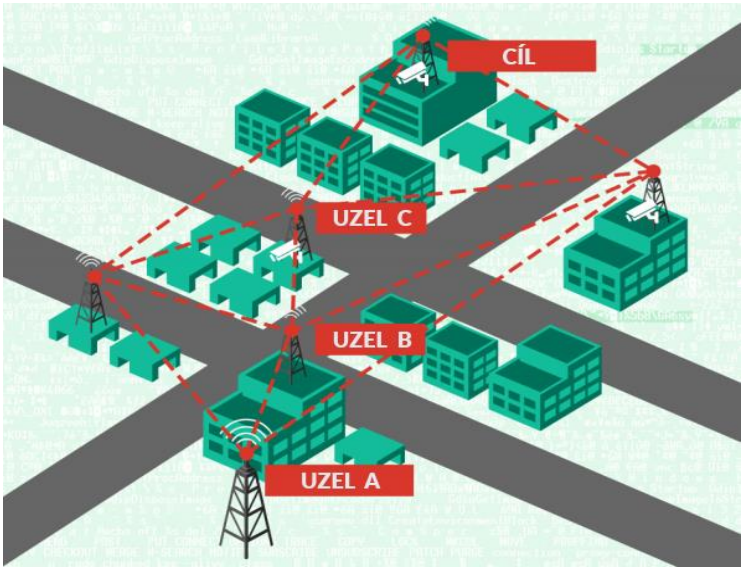
Bohužel i chytré popelnice se mohou stát terčem hackerského útoku. Pokud je použita centralizovaná platforma, útočník může manipulovat s popelářskými vozy a upravovat jejich trasu. V tomto případě je výchozím bodem útoku API řídicího systému.

Standard GSM používá 64-bitové A5/3 šifrování pro 3G sítě, které sice již bylo prolomeno, ale stále poskytuje ochranu proti běžnému odposlouchávání. V případě dostupnosti je možné použít lépe zabezpečený standard 4G LTE. Některé další chytré popelnice využívají pro komunikaci protokol LoRa WAN, zabezpečení tohoto protokolu již bylo popsáno v předchozí kapitole.

3.3.3.3 Veřejné bezpečnostní kamerové systémy

V návrhu je použit kamerový systém na bázi síťových kamer. Jak již bylo popsáno v kapitole 2.6, nezabezpečené IP kamery je možné velmi snadno zneužít. Používání nezabezpečeného CCTV systému je velmi nebezpečné a v některých případech až kontraproduktivní.

Při návrhu kamerového systému ve skutečnosti není až tak důležitý použitý hardware, ale jeho implementace a vhodné zabezpečení. Základem, stejně jako u většiny předchozích prvků, je použití šifrování a změna defaultních přihlašovacích údajů. Síťové kamerové systémy obvykle používají hvězdicovou topologii (Star Network), kdy jednotlivá zařízení (kamery) jsou připojena k centrálnímu hubu nebo routeru. To je velmi dobré řešení při použití na relativně krátkou vzdálenost, například v rámci budov. V případě komplexního systému pro celé město, je vhodné použít smíšenou topologii (Mesh Topology), ve které jsou některé uzly přímo propojeny s více než jedním dalším uzlem v síti.



Obrázek 15: Smíšená topologie CCTV systému

Zdroj: upraveno podle [16]

Obrázek 15 ilustruje cestu paketu, který je odeslaný z uzlu A, putuje přes uzly B a C až do cíle. Mezitím pakety odeslané z jiných uzlů cestují po úplně jiné trase a z toho důvodu nemohou být zachyceny při odposlouchávání na jediném místě. IP kamery mohou odesílat data a komunikovat se serverem pomocí protokolů TCP nebo UDP/RTP, záleží na výrobci a použité technologii.

Pro zabezpečení síťového kamerového systému je důležité zabezpečit jednotlivé kamery proti fyzickému narušení, použít šifrování a silné WPA heslo, nevysílat SSID a případně použít filtrování MAC adres. To by mělo zaručit rozumnou úroveň zabezpečení, která nebude omezovat funkčnost.

3.3.3.4 Veřejné Wi-Fi připojení

Zabezpečením Wi-Fi hotspotů se zabývá velká spousta prací, proto budou v této práci pouze uvedeny základní doporučení pro zabezpečení bezdrátové sítě v rámci Smart City.

Prvním krokem je zabezpečit síťové prvky proti fyzickému přístupu. V případě veřejného hotspotu je z hlediska zabezpečení vhodné použít autorizaci pomocí přihlašovací stránky a až poté umožnit uživatelům přístup k Internetu. Mnohem bezpečnější, avšak nepříliš uživatelsky přívětivé řešení, je hotspot zabezpečit pomocí WPA2 hesla a firewallu.

Připojením k veřejným a nezabezpečeným Wi-Fi hotspotům se každý uživatel vystavuje riziku. Na takových sítích nelze absolutně garantovat bezpečnost.

4 OBECNÁ DOPORUČENÍ PRO TVORBU SMART CITY

Útok na inteligentní technologie v kritických sektorech může mít na běžné každodenní činnosti zásadní negativní vliv. Absence bezpečnostních standardů může slibované výhody změnit v nepředvídatelné problémy. V této kapitole jsou proto uvedeny obecná bezpečnostní doporučení pro tvorbu chytrého města:

1. Výběr vhodného dodavatele

   Pří výběru dodavatele technologií je důležité zjistit podrobnosti nejen o nabízené technologii, ale také spolehlivosti samotného dodavatele. Zároveň je vhodné, aby smlouva s dodavatelem obsahovala doložku o bezpečnostním auditu, který bude proveden nejméně jednou ročně.

2. Kontrola kvality a provedení penetračních testů

   Inteligentní technologie se musí podrobit důkladné kontrole a testováním před samotnou implementací v celém městě. To umožňuje odhalení bezpečnostních rizik předtím, než jakákoliv služba nebo zařízení budou zpřístupněny veřejnosti. Pro testování je vhodné najmout nezávislé bezpečnostní techniky, kteří mohou technologie testovat pravidelně.

3. Zajištění údržby a pravidelných aktualizací softwaru

   Aktualizace softwaru musí být instalovány co nejdříve, zároveň se však obec musí ujistit, že aktualizace jsou dodávány v bezpečné formě – šifrované a digitálně podepsané.

4. Zpracování údajů s ohledem na soukromí uživatelů

   Veškerá data shromážděná systémy chytrého města by měla být anonymizována, aby bylo chráněno soukromí občanů.

5. Použití šifrování a autentizace

   Veškerá komunikace by měla být zabezpečena proti odposlechu a modifikaci, zejména pokud obsahuje citlivé informace. Toho lze docílit použitím silného šifrování a používáním šifrovacích klíčů k autentizaci

6. Zajištění kontinuity základních služeb

   V případě nenadálé situace, kdy všechny systémy selžou, je nezbytné občanům zaručit přístup k základním službám (elektrická energie, voda), ohlášení mimořádné události (tísňová volání) apod.

ZÁVĚR

Cílem této práce bylo identifikovat zranitelná místa konceptu Smart City a následně navrhnout vhodná bezpečnostní opatření. Otázka bezpečnosti chytrých měst je velmi složitá, nejen vzhledem ke komplexnosti celého konceptu, ale také proto, že neexistuje ucelená definice a doporučený postup pro implementaci. Použité technologie mohou pocházet od různých dodavatelů a nutně nemusí být mezi sebou kompatibilní. Při volbě chytrých řešení pro města je důležité se zabývat nejen konečnou cenou, ale také bezpečností použitých technologií.

Koncept využívá a kombinuje infrastrukturu IoT prvků, tudíž, stejně jako v jiných odvětvích, i zde platí, že každý systém je prolomitelný – závisí pouze na času, úsilí a finančních prostředcích. Nejzávažnější následky, při napadení technologií Smart City, hrozí v případě kritické infrastruktury, tedy oblastí energetiky a dopravy.

Samotné zabezpečení senzorů závisí dodavatelích, potažmo na výpočetním výkonu zařízení, který je obvykle omezený z důvodu nízké hmotnosti. Při zabezpečování přenosových cest již nejsou možnosti tolik omezené a lze použít technologie a protokoly umožňující ověření autenticity, integrity a důvěrnosti přenášených dat. Jako nejslabší a nejrizikovější článek bezpečnosti lze považovat lidský faktor, v případě ignorování bezpečnostních doporučení (např. změna defaultních přihlašovacích údajů), má útočník vysokou šanci na úspěšné provedení útoku.

V této práci byly navrženy možnosti zabezpečení vybraných senzorových prostředků z oblastí dopravy, energetiky a prostředí. Získané poznatky a postupy, včetně závěrečných doporučení, mohou být využity menšími městy pro implementaci a zabezpečení zmíněných technologií.

Na závěr si dovolím uvést české přísloví: „Oheň je dobrý sluha, ale zlý pán.“ V podobném duchu lze totiž hovořit i o technologiích konceptu Smart City, proto je nezbytné, aby rizika související s jejich používáním byla co nejmenší.

POUŽITÁ LITERATURA

[1] Airly: What's in the air you breathe? [online]. [cit. 2018-03-25]. Dostupné z: https://airly.eu/

[2] ALLWINKLE, Sam a Peter CRUICKSHANK. Creating Smart-er Cities: An Overview. Journal of Urban Technology [online]. 2011, 18(2), 1-16 [cit. 2018-04-17]. DOI: 10.1080/10630732.2011.601103. ISSN 1063-0732. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/10630732.2011.601103

[3] ANAND, Priya. The 'Mind-Boggling' Risks your City Faces from Cyber Attackers [online]. 30 January 2016 [cit. 2018-02-15]. Dostupné z: https://www.marketwatch.com/story/the-mind-boggling-risks-your-city-faces-from-cyber-attackers-2016-01-04

[4] BÁRTA, David, et al. Metodika Konceptu inteligentních měst: Projekt TB930MMR001 [online]. 22.3. 2015. Brno, 2015 [cit. 2018-03-01]. Dostupné z: http://www.strukturalni-fondy.cz/getmedia/9c597c78-8651-43a8-8d94-bc9f19da74c5/TB930MMR001_Metodika-konceptu-Inteligentnich-mest-2015.pdf

[5] BHARDWAJ, Mohit. IoT device security: a comprehensive look, from edge to cloud [online]. In: 22 September 2017 [cit. 2018-02-15]. Dostupné z: http://www.ioti.com/security/iot-device-security-comprehensive-look-edge-cloud

[6] Bigbelly: Smart City Solutions [online]. [cit. 2018-03-25]. Dostupné z: http://Bigbelly.com

[7] CACCIATORE, Giuseppe, Claudio FIANDRINO, Dzmitry KLIAZOVICH, Fabrizio GRANELLI a Pascal BOUVRY. Cost analysis of smart lighting solutions for smart cities. In: 2017 IEEE International Conference on Communications (ICC) [online]. IEEE, 2017, 2017, [cit. 2018-03-21]. DOI: 10.1109/ICC.2017.7996886. ISBN 978-1-4673-8999-0. Dostupné z: http://ieeexplore.ieee.org/document/7996886/

[8] CAMHI, Jonathan. BI Intelligence projects 34 billion devices will be connected by 2020. Business Insider [online]. 6 November 2015 [cit. 2018-02-27]. Dostupné z: http://www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11

[9] CERRUDO, Cesar. Hacking US (and UK, Australia, France, etc.) Traffic Control Systems [online]. WEDNESDAY, APRIL 30, 2014 [cit. 2018-04-04]. Dostupné z: http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html

[10] CISCO. Intelligent Public Transportation [online]. In: . [cit. 2018-03-17]. Dostupné z: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/trans/intelligent_public_transportation.pdf

[11] Cyber Security: a necessary pillar of Smart Cities [online]. 2016 [cit. 2018-02-14]. Dostupné z: http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf

[12] ENDORF, Carl F., Eugene SCHULTZ a Jim MELLANDER. Detekce a prevence počítačového útoku. Praha: Grada, 2005. ISBN 80-247-1035-8.

[13] FOSTER, James C. Hacking - Buffer Overflow: [zneužití, detekce a prevence]. Praha: Grada, 2007. ISBN 978-80-247-1480-6.

[14] GARFIELD, Leanna. South Korea is building a $35 billion city designed to eliminate the need for cars [online]. 14 February 2018 [cit. 2018-03-25]. Dostupné z: http://www.businessinsider.com/songdo-south-korea-design-2017-11

[15] GOODMAN, Marc. Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. [online]. Anchor, 2015 [cit. 2018-02-15]. Dostupné z: http://executivebookreview.com/wp-content/uploads/2017/04/Future-Crimes.pdf

[16] HIOUREAS, Vasili a Thomas KINSEY. Does CCTV put the public at risk of cyberattack?: How insecure surveillance technology is working against you [online]. In: . [cit. 2018-04-06]. Dostupné z: https://securingsmartcities.org/wp-content/uploads/2015/05/CCTV_research_final.pdf

[17] Chytrá města: Jak efektivněji spravovat město a zvyšovat kvalitu života jeho obyvatel [online]. Siemens, s.r.o [cit. 2018-04-07]. Dostupné z: siemens.cz/chytramesta

[18] International Electrotechnical Commission. Smart Cities [online].[cit. 2018-02-13]. Dostupné z: http://www.iec.ch/about/brochures/pdf/technology/smartcities.pdf

[19] IoT Attack Surface Areas. In: Open Web Application Security Project [online]. 29 November 2015 [cit. 2018-02-17]. Dostupné z: https://www.owasp.org/index.php/IoT_Attack_Surface_Areas

[20] KITCHIN, Rob a DODGE Martin. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. Journal of Urban Technology [online]. 2017, , 1-19 [cit. 2018-02-15]. DOI: 10.1080/10630732.2017.1408002. ISSN 1063-0732. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/10630732.2017.1408002

[21] KREBS, Brian. KrebsOnSecurity Hit With Record DDoS. Krebs On Security [online]. 16 September 2016 [cit. 2018-02-27]. Dostupné z: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[22] MAHMOUD, Rwan, Tasneem YOUSUF, Fadi ALOUL a Imran ZUALKERNAN. Internet of things (IoT) security: Current status, challenges and prospective measures. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) [online]. IEEE, 2015, 2015, , 336-341 [cit. 2018-02-15]. DOI: 10.1109/ICITST.2015.7412116. ISBN 978-1-9083-2052-0. Dostupné z: http://ieeexplore.ieee.org/document/7412116/

[23] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. Hacking bez záhad. Praha: Grada, 2007. ISBN 978-80-247-1502-5.

[24] MCNAMARA, Patrick. Defining a Smart Energy City. The World's Smart Cities Organization [online]. February 20, 2017 [cit. 2018-04-14]. Dostupné z: http://wsco-online.com/2017/02/20/defining-a-smart-energy-city/

[25] MILLER, Robert. LoRa Security: Building a Secure LoRa Solution[online]. In: . MWR Labs Whitepaper [cit. 2018-04-01]. Dostupné z: https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf

[26] NANNI, Giampiero. Transformational Smart Cities: cyber security and resilience. [online]. Symantec Corporation, 2013. Dostupné z: https://www.symantec.com/connect/blogs/transformational-smart-cities-cyber-security-and-resilience

[27] PRINCE, Brian. Almost 70 Percent of Critical Infrastructure Companies Breached in Last 12 Months: Survey [online]. 14 July 2014 [cit. 2018-02-15]. Dostupné z: https://www.securityweek.com/almost-70-percent-critical-infrastructure-companies-breached-last-12-months-survey

[28] Řízení dopravy. CROSS Zlín a.s. [online]. [cit. 2018-03-17]. Dostupné z: http://www.cross.cz/cs/produkty-rizeni-dopravy

[29] SEDLÁK, Jan. a jede se dál. Praha za miliony pořizuje chytré popelnice hlásící se přes cloud. Lupa.cz [online]. 7. 8. 2017 [cit. 2018-04-02]. Dostupné z: www.lupa.cz/clanky/a-jede-se-dal-praha-za-miliony-porizuje-chytre-popelnice-hlasici-se-pres-cloud

[30] SHARMA, Sumit. Planning an architecture for the Internet of Things [online]. In: . 5 November, 2014 [cit. 2018-04-14]. Dostupné z: https://www.slideshare.net/sumitcan/iot-architecture

[31] SIEMENS AG. Intelligent City Parking Solutions: Advanced traffic management for your smart city [online]. In: . Germany, 2016 [cit. 2018-03-17]. Dostupné z: https://www.mobility.siemens.com/mobility/global/SiteCollectionDocuments/en/road-solutions/urban/smart-parking/smart-parking-brochure.pdf

[32] Skupina ČEZ dokončila výběr dodavatele prvních inteligentních měřidel [online]. [cit. 2018-03-21]. Dostupné z: https://www.cez.cz/cs/pro-media/tiskove-zpravy/3003.html

[33] SWIMMER Morton, Akira URANO, Stephen HILT, Rainer VOSSELER a Philippe LIN. Securing Smart Cities: Moving Toward Utopia with Security in Mind [online]. 2017 [cit. 2018-02-13]. Dostupné z: https://documents.trendmicro.com/assets/wp/wp-securing-smart-cities.pdf

[34] Understanding energy usage starts at home [online]. In: . [cit. 2018-03-21]. Dostupné z: https://energyathaas.wordpress.com/2014/01/01/understanding-energy-usage-starts-at-home/

[35] WEISER, Mark, Rich GOLD a John BROWN. The origins of ubiquitous computing research at PARC in the late 1980s. IBM SYSTEMS JOURNAL [online]. 1999(VOL 38), 693-696 [cit. 2018-03-25]. Dostupné z: http://www.cs.cmu.edu/~jasonh/courses/ubicomp-sp2007/papers/03-weiser-origins.pdf