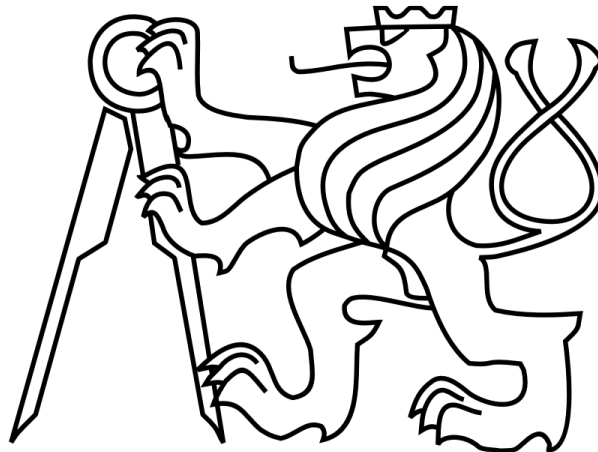


České vysoké učení technické v Praze

Fakulta elektrotechnická

Katedra telekomunikační techniky



**MACHINE-TO-MACHINE (M2M) KOMUNIKACE PROSTŘEDNICTVÍM
VEŘEJNÝCH KOMUNIKAČNÍCH SÍTÍ**

**MACHINE-TO-MACHINE (M2M) COMMUNICATION BY MEANS OF
PUBLIC COMMUNICATIONS NETWORKS**

BAKALÁŘSKÁ PRÁCE

Rok: 2017/2018

Autor: Andrea Stejskalová

Vedoucí práce: Ing. Zdeněk Brabec, CSc.

Studijní program: Komunikace, multimédia a elektronika

Studijní obor: Síťové a informační technologie

Čestné prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracovala sama s přispěním vedoucího na základě literatury a pramenů uvedených v práci. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

V Praze dne:

.....

Poděkování

Chtěla bych poděkovat zejména Ing. Zdeňkovi Brabcovi, CSc. za vedení této práce, pravidelné schůze a konzultace ohledně práce. Poděkování patří také mojí rodině, která mě podporovala po celou dobu mého studia i při psaní této bakalářské práce.

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Stejskalová** Jméno: **Andrea** Osobní číslo: **456889**
Fakulta/ústav: **Fakulta elektrotechnická**
Zadávající katedra/ústav: **Katedra telekomunikační techniky**
Studijní program: **Komunikace, multimédia a elektronika**
Studijní obor: **Sít'ové a informační technologie**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Machine-to-machine (M2M) komunikace prostřednictvím veřejných komunikačních sítí

Název bakalářské práce anglicky:

Machine-to-machine (M2M) communication by means of public communications networks

Pokyny pro vypracování:

Internet věcí (IoT) je tvořen soustavou tzv. inteligentních objektů, mezi nimiž probíhá přenos informací nazývaný Machine-to-Machine (M2M) komunikace. Definujte základní pojmy z oblasti M2M a popište vazby mezi nimi. Zpracujte přehled používaných technologií. Hlavním cílem práce je rozbor možností využití veřejných komunikačních sítí pro M2M komunikaci, jehož součástí bude i analýza trhu v této oblasti a predikce jeho vývoje do r. 2030.

Seznam doporučené literatury:

- [1] Doporučení ITU-T z řady Y.4000-Y.4999: Internet of things and smart cities and communities. Dostupné z: <https://www.itu.int/itu-t/recommendations/index.aspx?ser=Y> [on-line]
- [2] Internet Society. White Paper: The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World. Dostupné z: <https://www.internetsociety.org/resources/doc/2015/iot-overview> [on-line]
- [3] Otevřená data Českého telekomunikačního úřadu. Ukazatele o trhu mobilních sítí. Dostupné z: <http://data.ctu.cz/dataset/ukazatele-o-trhu-mobilnich-siti/resource/bd3a0fb7-e81e-48b1-9587-99a9d51f5c07> [on-line]

Jméno a pracoviště vedoucí(ho) bakalářské práce:

Ing. Zdeněk Brabec, CSc., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **22.01.2018** Termín odevzdání bakalářské práce: **25.05.2018**

Platnost zadání bakalářské práce: **30.09.2019**

Ing. Zdeněk Brabec, CSc.
podpis vedoucí(ho) práce

podpis vedoucí(ho) ústavu/katedry

prof. Ing. Pavel Ripka, CSc.
podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Studentka bere na vědomí, že je povinna vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

Datum převzetí zadání

Podpis studentky

ANOTACE

Cílem bakalářské práce „Machine-to-Machine (M2M) komunikace prostřednictvím veřejných komunikačních sítí“ je definovat a popsat komunikace mezi stroji, kde nejdůležitější roli hraje popis internetu věcí, který se pro tento typ komunikace využívá. Internet věcí definujeme podle jeho základní charakteristiky a určitých požadavků. Pro přesnější popis si popíšeme referenční model internetu věcí a poté porovnáme s platformou M2M. Další důležité téma je aplikační programovací rozhraní, které umožňuje lepší přístup ke službám a zařízením internetu věcí v komunikační síti. Pro nás nejdůležitější komunikační síť je mobilní síť, která je využívána v M2M komunikaci. Mobilní sítě můžeme rozdělit na licencované nebo nelicencované. Oba typy mobilních sítí jsou využity v M2M komunikaci. Komunikace mezi stroji začíná být čím dál více rozšířenější a expandují do více oblastí trhu. Podle celosvětové či evropské predikce se bude komunikace mezi stroji nadále rozvíjet do dalších oblastí a počet využití se bude zvětšovat. Se stejným trendem můžeme počítat i v České Republice.

Klíčová slova: M2M komunikace, Internet věcí, LPWAN, predikce M2M

ANNOTATION

This bachelor thesis "Machine-to-Machine (M2M) communication by means of public communications networks" focuses on concept of the Internet of Things. It defines and describes this concept as a communication which is existing among machines. To better understand this concept, I specify core characteristics and assumptions for IoT. In this instance I use some important issues like, reference model of IoT his comparison with M2M platform. Other is API, Application Programming Interface, which secure better access to services and devices of IoT in communication network. Mobile network as a part of communication network is crucial for this thesis, because it is used within M2M communication. Communication among machines is starting to be common thing and it expands to all corners of business and markets. Regarding this rising significance, I present market predictions for usage of communication among devices in Europe and Czech Republic.

Key words: M2M communication, Internet of Things, LPWAN, prediction for M2M

Obsah

1	ÚVOD	1
2	INTERNET VĚCÍ	2
2.1	FYZICKÝ A INFORMAČNÍ SVĚT	3
2.2	ZAŘÍZENÍ	4
2.3	BRÁNY PRO APLIKACE INTERNETU VĚCÍ	5
2.4	ZÁKLADNÍ CHARAKTERISTIKA IoT	6
2.5	POŽADAVKY IoT	7
2.6	POUŽITÍ	9
2.7	REFERENČNÍ MODEL INTERNETU VĚCÍ	11
3	M2M	13
3.1	M2M REFERENČNÍ MODEL	14
3.2	ARCHITEKTONICKÝ RÁMEC VRSTVY M2M	15
3.3	REFERENČNÍ BODY	16
4	API A PROTOKOLY	17
4.1	VYUŽITÍ API	18
5	TELEKOMUNIKAČNÍ SÍŤ	19
5.1	MOBILNÍ SÍŤ A 3GPP	19
5.2	ROZSÁHLÁ SÍŤ S NÍZKOU SPOTŘEBOU	20
5.2.1	LICENCOVANÉ LPWAN	20
5.2.2	NELICENCOVANÉ LPWAN	22
6	TRH	23
6.1	PREDIKCE TRHU	24
6.1.1	AKTIVNÍ SIM	24
6.1.2	M2M	25
6.1.3	eCALL	33
6.2	POROVNÁNÍ	34
7	ZÁVĚR	35
8	POUŽITÁ LITERATURA	36

SEZNAM POUŽITÝCH ZKRATEK

M2M	Machine-to-Machine
IoT	Internet of Things
LPWA	Low-Power Wide-Area
SIM	Subscriber Identity Module
GPRS	General Packet Radio Service
ITU	International Telecommunications Union
PnP	Plug and Play
CAN	Controller Area Network
PSTN	Public Switched Telephone Network
3G/4G	3 Generation/ 4 Generation
LTE	Long Term Evolution
DSL	Digital Subscriber Line
IP	Internet Protocol
D-SL	Device-Service Layer
G-SL	Gate – Service Layer
NA-SL	Network Application – Service Layer
SL-SL	Service Layer – Service Layer
NAT-PMP	Network Address Translation Port Mapping Protocol
DPWS	Device Profile for Web Services
SOAP	Simple Object Access Protocol
HTTP	Hypertext Transfer Protocol
NCE	Network Capability Exposure
3GPP	The 3rd Generation Partnership Project
WiMAX	Worldwide Interoperability for Microwave Access
GSM	Global System for Mobile
NB IoT	NarrowBand Internet of Things
WCDMA	Wideband Code Division Multiple Access
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network
MMS	Multimedia Messaging Service
ARC	Alarm Receiving Centre
POS	Point of Sale/ Point of Service
mPOS	Mobile Point of Sale
LTE-M	Long Term Evolution for Machines
EC-GSM	Extended Coverage Global System for Mobile

SEZNAM OBRÁZKŮ

Obrázek 1 - Nová dimenze komunikace pro Internet věcí[2]	2
Obrázek 2 - Komunikace ve fyzickém a informačním světě[2].....	3
Obrázek 3 - Typy zařízení a jejich vztahy s fyzickými věcmi[2].....	4
Obrázek 4 - Typický rozmístění brány pro aplikace IoT[4].....	5
Obrázek 5 - Obecný případ využití Internetu věcí[8].....	9
Obrázek 6 - Referenční model pro Internet věcí[2].....	11
Obrázek 7 - Porovnání M2M a IoT[11]	13
Obrázek 8 - Referenční model M2M a vyobrazení referenčních bodů[13]	14
Obrázek 9 - Architektonický rámec v M2M vrstvě služeb[13].....	15
Obrázek 10 - Referenční body v referenčním modelu M2M[13].....	16
Obrázek 11 - Přehled síťových využití pro Internet věcí[16].....	18

SEZNAM GRAFŮ

Graf 1 - Predikce počtu SIM bez M2M.....	24
Graf 2 - Penetrace aktivních SIM karet.....	24
Graf 3 - Predikce počtu M2M SIM pro sledovací systémy.....	25
Graf 4 - Predikce počtu M2M SIM pro smart metery	26
Graf 5 - Predikce počtu M2M SIM pro zabezpečovací systémy.....	27
Graf 6 - Predikce počtu M2M SIM pro GPRS terminály.....	28
Graf 7 - Predikce počtu M2M SIM pro bezdrátová zařízení v zemědělství.....	29
Graf 8 - Predikce počtu M2M SIM pro autonomní auta	30
Graf 9 - Predikce počtu M2M SIM pro ostatní odvětví	31
Graf 10 - Predikce počtu všech M2M SIM	31
Graf 11 - Penetrace M2M SIM.....	31
Graf 12 - Predikce počtu všech SIM karet	32
Graf 13 - Penetrace SIM karet (Aktivní i M2M).....	32
Graf 14 - Predikce systémů eCall.....	33
Graf 15 - Predikce trhu.....	34
Graf 16 - Predikce trhu podle mých hodnot	34

SEZNAM TABULEK

Tabulka 1 - Počet SIM dle ČTÚ.....	23
------------------------------------	----

1 ÚVOD

Ve světě dochází ke stálým automatizacím a technologickým pokrokům. Přirozeně se člověk snaží vymyslet koordinaci s okolními věcmi čím dál jednodušší a zároveň preciznější. Jedním z velkých pokroků došlo při využití komunikace mezi zařízeními, kde hlavní výhodou je komunikace probíhající právě mezi stroji, bez jakéhokoliv osobního zásahu člověka. Na tomto způsobu je založena jak komunikace M2M, tak i pokročilejší technologie Internet věcí. M2M je zkratka pro Machine-to-Machine a jedná se o komunikaci mezi stroji. Pro důkladnější popis funkcí internetu věcí nebo M2M komunikace využijeme referenční model, který je pro obě dvě technologie dosti podobný. V obou případech se referenční model dělí na čtyři základní vrstvy, mezi které patří vrstva aplikační, vrstva pro podporu služby a aplikace, síťová vrstva a vrstva zařízení. Komunikace mezi stroji využívá v referenčním modelu referenční body pro komunikaci mezi danými stroji a tím se liší od internetu věcí. Internet věcí je vlastně systém, kde více zařízení komunikuje mezi sebou prostřednictvím senzorů či digitální konektivity. Na rozdíl od toho řešení M2M vyloženě obsahují lineární komunikační kanál mezi danými stroji. M2M komunikace i Internet věcí mají ale další společnou důležitou věc a tím je využívaná síť. Pro oba typy technologie je zapotřebí rozsáhlá telekomunikační síť s nízkou spotřebou. Termín LPWA, rozsáhlé telekomunikační sítě s nízkou spotřebou, zahrnuje standardizované buněčné sítě, které pracují v licencovaném pásmu, ale i sítě, které pracují v pásmu nelicencované. Přestože se technologie M2M i IoT stále vyvíjejí a zdokonalují, na trhu jsou v různých odvětvích již využívány. Možná se dá říct, že již ve všech odvětvích. Ve světě již mají velké zastoupení v mnoha sektorech. Na českém trhu již všichni operátoři nabízejí M2M SIM karty. Nejčastěji se s využitím komunikace strojů bez zásahu člověka setkáme v průmyslu, zejména automobilovém. V tomto průmyslu se začínalo od systému na sledování polohy služebních aut a dostáváme se až k polo-automatizovaným vozidlům, kde v plánu jsou v budoucnu až plně automatizovaná. Ulehčení a zrychlení práce nastává také v sektorech jako je bankovníctví, energetika, zemědělství a mnoha dalších. V bankovníctví využíváme M2M SIM karet v bezdrátových GPRS terminálech. V energetice došlo k ulehčení práce jak pro uživatele, tak pro dodavatele zavedením chytrých měřičů elektrické energie nebo plynu. V zemědělství je již několik strojů, který využívají M2M komunikaci. Pro člověka vždy byla a vždy bude důležitá jeho vlastní bezpečnost, proto v tomto směru dochází nadále k pokroku a samozřejmě i zde je využití M2M, kde M2M SIM jsou zavedeny přímo do zabezpečovacích systémů využitých v domech, bytech, kancelářích či ostatních objektech. Každý od spotřebitelů až po podnikatele postupně přijímá změny ohledně internetu věcí a M2M komunikace.

2 INTERNET VĚCÍ

Poprvé byl termín Internet věcí použit Kevinem Ashtonem v roce 1999. Ten popisuje systém, ve kterém by objekty ve fyzickém světě mohly být připojeny k internetu prostřednictvím senzorů. Koncept internetu věcí se tak začíná formulovat jako široké spektrum síťových produktů, systémů a senzorů, které využívají pokrok v oblasti výpočetní vědy, síťovém propojení a miniaturizaci elektroniky.

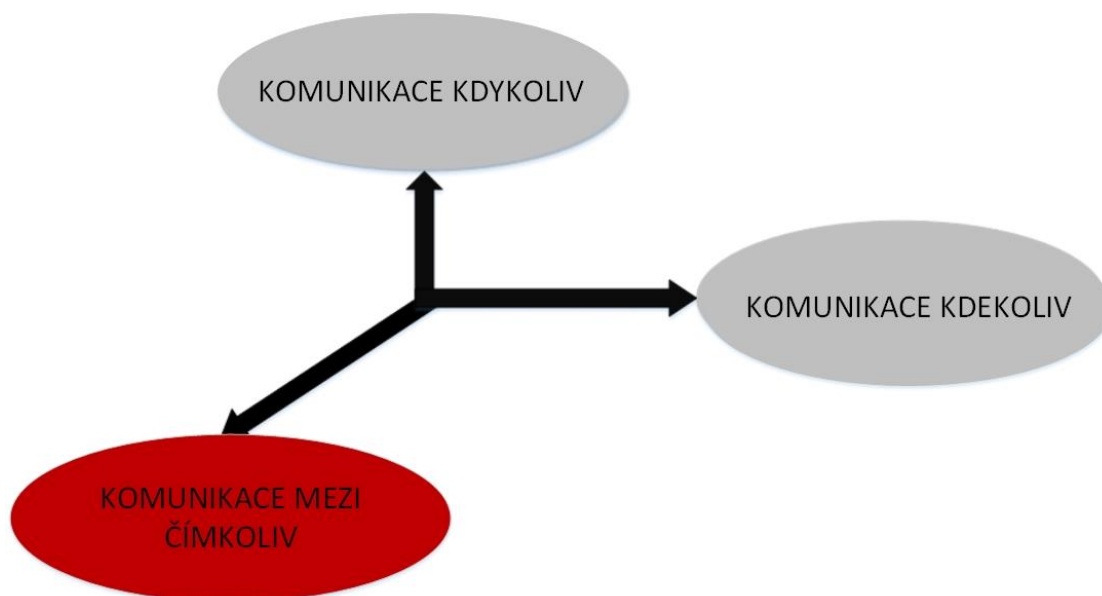
Aktuálnější definice internetu věcí podle ITU-T z roku 2012 Recommendation Y.2060 zní:

Internet věcí: je globální infrastruktura pro společnost informace, umožňující pokročilejší služby a propojení (fyzických a virtuálních) věcí na základě existujících a vyvíjejících se vnitřních informačních a komunikačních technologií.

Poznámka 1 - prostřednictvím možnosti využívání, identifikace, získávání dat, zpracovávání a komunikace, Internet věcí umožňuje plně využívat služeb pro nejrůznější druhy aplikací, zatímco zajišťuje bezpečnost a soukromí.

Poznámka 2–Z širší perspektivy lze na Internet věcí nahlížet jako na vizi s technologickými a sociálními dopady.[1]

Základem IoT technologie byly a jsou dvě dimenze. První je komunikace probíhající kdykoliv, což znamená že musí být dostupná celý den, jak v noci, tak i přes den. Další podmínkou je využití komunikace kdekoliv. Možnost komunikace lze využít jak za pomoci počítače, tak i bez něj. Novou dimenzí je komunikace mezi čímkoliv. Mezi základní čtyři varianty komunikace patří, komunikace mezi počítači, komunikace mezi lidmi, komunikace mezi věcmi a komunikace mezi člověkem a věcí. Za věc se považuje předmět fyzického světa (fyzických věcí) nebo světa informací (virtuálních věcí), které lze identifikovat a integrovat do komunikačních sítí.



Obrázek 1 - Nová dimenze komunikace pro Internet věcí[2]

2.1 FYZICKÝ A INFORMAČNÍ SVĚT

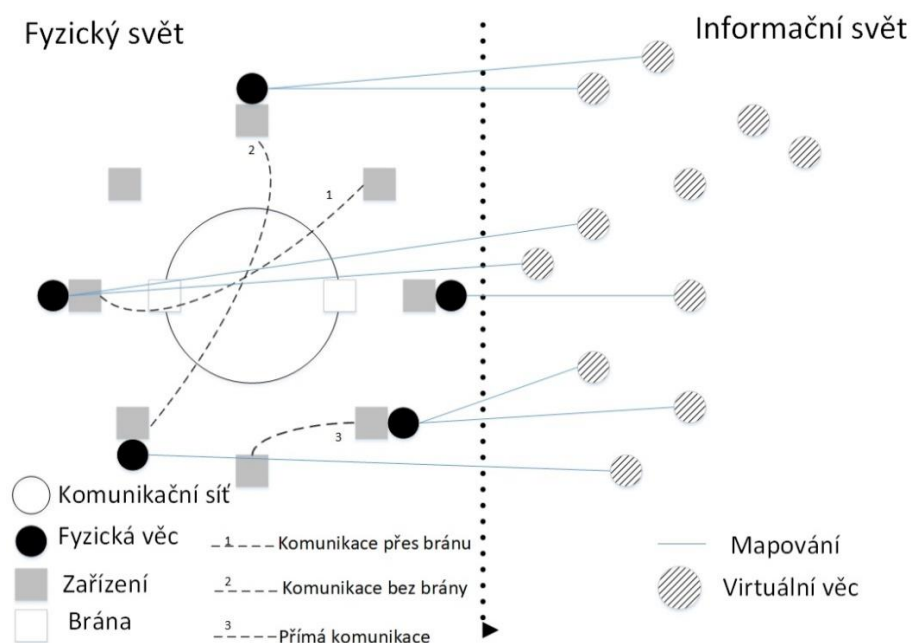
Důležité pro Internet věcí, je definovat co vlastně věc v tomto spojení znamená. Máme dva druhy věcí, kde prvním příkladem jsou věci fyzické a druhým věci virtuální.

Fyzické věci existují ve fyzickém světě a jsou schopny být snímány, aktivovány a připojeny. Příkladem fyzických věcí je okolní prostředí, průmysloví roboti, zboží a elektrická zařízení.

Virtuální věci existují v informačním světě a mohou být uloženy, zpracovány a zpřístupněny. Virtuální věci zahrnují multimediální obsah a aplikační software. Fyzická věc může být reprezentována v informačním světě prostřednictvím jedné nebo více virtuálních věcí (mapování), ale virtuální věc může existovat i bez jakékoli fyzické záležitosti.

„Fyzický svět bude do značné míry ovlivněn informačním světem. Znalosti a schopnosti informačního světa rozšiřují místní znalosti a schopnosti fyzických věcí a přinášejí uživatelům nepředstavitelné zkušenosti.“

[1]



Obrázek 2 - Komunikace ve fyzickém a informačním světě[2]

Zařízení ve fyzickém světě jsou zařízení s povinnými komunikačními schopnostmi a volitelnými schopnostmi snímání, ovládání, sběru dat, ukládání dat a zpracování dat.

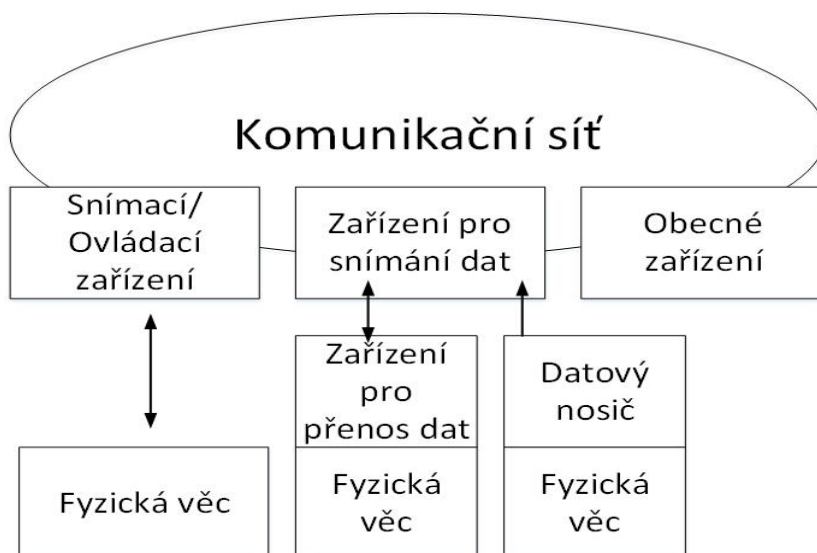
Přestože na obrázku 2 jsou zobrazeny pouze interakce ve fyzickém světě (komunikace mezi zařízeními), interakce probíhají také v informačním světě (výměna mezi virtuálními věcmi) a mezi fyzickým světem a informačním světem (výměna mezi fyzickými věcmi a virtuálními věcmi).

Jsou tři druhy komunikací mezi zařízeními. Komunikace prostřednictvím komunikační sítě přes bránu (případ 1), přes komunikační síť bez brány (případ 2) nebo přímo, to znamená bez použití komunikační sítě (případ 3). Také jsou možné kombinace případů, například zařízení mohou komunikovat s jinými zařízeními pomocí přímé komunikace prostřednictvím lokální sítě.

2.2 ZAŘÍZENÍ

Pro fyzický svět jsou důležité nejen fyzické věci, ale s nimi spjaté i zařízení. Jejich úkolem je sbírání různých druhů informací a poskytování je informačním a komunikačním sítím pro další zpracování. Některá zařízení také provádějí operace založené na informacích získaných z informačních a komunikačních sítí.

Na obrázku 3 můžeme vidět různé typy zařízení a vztah mezi zařízeními a fyzickými věcmi.



Obrázek 3 - Typy zařízení a jejich vztahy s fyzickými věcmi[2]

V komunikační síti máme tři základní druhy zařízení, mezi které patří snímací/ovládací zařízení, zařízení pro zachycování dat a obecné zařízení. [1]

Prvním druhem zařízení je zařízení pro přenos, které slouží pro nepřímé propojení fyzické věci ke komunikační síti. Všechna zařízení musí splňovat minimální komunikační požadavky v internetu věcí. Snímací a ovládací zařízení mohou detekovat nebo měřit informace související s okolním prostředím a převést je na digitální elektronické signály. Mohou také převádět digitální elektronické signály z informačních sítí do provozu. Obecně platí, že snímací a ovládací zařízení vytvářejí lokální síť, které komunikují navzájem pomocí kabelového nebo bezdrátového připojení.

Zařízení pro zachycování dat jsou čtečky nebo zapisovače, které mají schopnost interagovat s fyzickými věcmi. Interakce se může stát nepřímo prostřednictvím zařízení pro přenos dat nebo přímo prostřednictvím datových nosičů. V prvním případě zařízení pro zachycování dat čte informace o zařízení pro přenos dat a může volitelně také zapisovat informace dané komunikačními sítěmi na datové nosiče. Druhým případem je propojení datového nosiče s fyzickými věcmi a zahrnují vysokofrekvenční, infračervené, optické a galvanické řízení.

Obecné zařízení má možnosti zpracování a komunikace. Komunikovat může s technologiemi pomocí kabelové nebo bezdrátové komunikační sítě. Mezi obecná zařízení patří například průmyslové stroje, domácí spotřebiče a chytré telefony. Obecné zařízení je i fyzická věc.

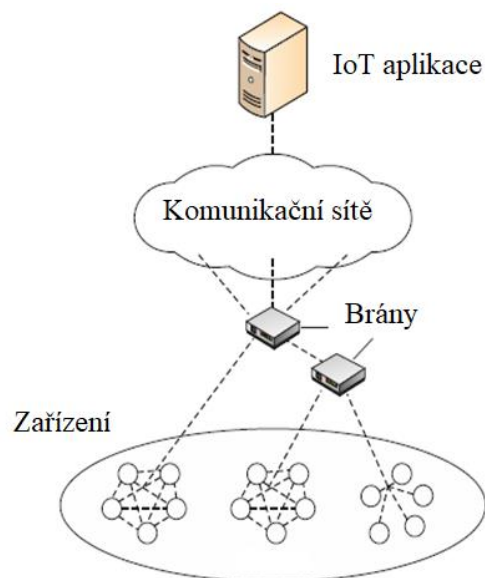
2.3 BRÁNY PRO APLIKACE INTERNETU VĚCÍ

Pro podporu propojení zařízení s komunikačními sítěmi v rámci internetu věcí jsou důležité brány, které dále provádí potřebný překlad mezi protokoly, které používají zařízení a mezi protokoly, které používají komunikační síť. Brána zachycuje data ze zařízení a přenáší data do aplikací. Dochází ke spojení různých typů zařízení s komunikačními sítěmi za pomoci jedné nebo více bran. Propojení mezi zařízeními a samostatnými branami může být různými způsoby, jak kabelově, tak i bezdrátově.[3]

Co se týče přizpůsobivosti, má brána obecnou charakteristiku přizpůsobivosti, kde se očekává, že rozhraní brány je standardizované. K bráně může přistupovat několik zařízení. Pro zvýšení rozšiřitelnosti brány je nutné, aby brána byla škálovatelná z hlediska počtu připojených zařízení a musí podporovat propojení s dalšími branami. Brána podporuje nejen různé zařízení, ale i různá schémata adresování. Brána musí hlídat přístup k zařízením i k sobě samotné a musí chránit soukromí dat, pro správné zabezpečení aplikací.

Brána je nezbytná součástí jako síťový most mezi zařízením a komunikační sítí. Komunikace alespoň s jednou aplikací musí být podporováno branou. Brána podporuje připojení několika zařízení a komunikačních technologií, proto brána musí být schopna vybrat příslušnou komunikační technologii podle specifických požadavků.

Ukládání dat v bráně je možné dvěma způsoby, dočasně nebo trvale. Trvale uložená data jsou důležitá pro provozní operace a správný výkon brány nebo zařízení. Data v branách a aplikacích by měla být uložena pevně a neporušitelně, pro bezpečnost a ochranu dat. Data uložena dočasně se odstraňují podle předem definovaných zásad.



Obrázek 4 - Typický rozmístění brány pro aplikace IoT[4]

Při interakci brány s aplikacemi se využívá aplikační logika. To znamená, že brána může funkce související s aplikací zpracovávat místně a nezávisle na zařízeních, která jsou vzdálená. Příkladem je zpracování a analýza dat před samotným přenosem.

2.4 ZÁKLADNÍ CHARAKTERISTIKA IoT

Internet věcí je popsán příslušnými charakteristikami. Mezi základní charakteristiky internetu věcí patří propojení, služby související s věcmi, heterogenita, dynamické změny a enormní měřítko.

Důležitou charakteristikou je propojení. Propojit se může vše s globální informační a komunikační infrastrukturou.

IoT je schopno poskytovat služby související s věcmi v rámci omezení věcí, jako je ochrana soukromí a sémantická konzistence mezi fyzickými věcmi a jejich přidruženými virtuálními věcmi. V tomto případě se změní technologie ve fyzickém, tak informačním světě.[1]

Přístroje v internetu věcí jsou heterogenní, což znamená, že jsou založeny na různých hardwarových platformách a sítích. Mohou komunikovat prostřednictvím různých sítí s jinými zařízeními nebo servisními platformami.

Dynamicky se může měnit počet zařízení nebo jejich stav. Stav zařízení se dynamicky mění, jako je například spánek a probuzení, připojení a odpojení, jakož i kontext zařízení, včetně umístění a rychlosti.

Vzhledem k budoucímu vývoji se dá očekávat, že počet zařízení, které je třeba spravovat a která budou spolu komunikovat, bude mít větší rozsah než zařízení připojená ke stávajícímu internetu. Poměr komunikace spouštěné zařízeními ve srovnání s komunikací vyvolanou lidmi se výrazně posune směrem ke komunikaci vyvolané zařízeními. Kritická bude správa vytvořených dat a jejich interpretace pro aplikační účely. To se týká sémantiky dat, stejně jako efektivní zpracování dat.

2.5 POŽADAVKY IoT

Aby IoT mohl vytvářet komplexní strukturu, jejichž prvky se dále specializují a zdokonalují, tak musí splňovat základní podmínky. Mezi požadavky na vysoké úrovni v internetu věcí patří konektivita založená na identifikaci, schopnost různých systémů vzájemně spolupracovat a poskytovat si služby, autonomní síťování, poskytování autonomních služeb, schopnosti na základě polohy, zabezpečení, ochrana soukromí, vysoce kvalitní a vysoce zabezpečené služby související s lidským tělem, ovladatelnost a plug and play (zapoj a hraj).

U konektivity založené na identifikaci je důležité propojení mezi věcí a internetem věcí, které je založeno na identifikátoru věci. Identifikátor je řada číslic, znaků a symbolů nebo jakákoli jiná forma údajů používaná k identifikaci účastníků, uživatelů, prvků sítě, funkcí nebo síťových entit poskytujících služby.[5] Identifikátory mohou být použity pro registraci nebo autorizaci. Mohou být buď veřejné do všech sítí, sdílené mezi omezeným počtem sítí nebo soukromé do určité sítě (soukromé ID se obvykle nezveřejňují třetím stranám). To také zahrnuje, že případné heterogenní identifikátory různých věcí se zpracovávají jednotným způsobem. Před každou komunikací je důležitá jedinečná identifikace, jako je například aplikace sensorových sítí a aplikace M2M. Aplikace M2M (Machine-to-Machine) je forma datové komunikace mezi dvěma nebo více entitami, v nichž alespoň jedna entita nutně nevyžaduje lidskou interakci nebo zásah do procesu komunikace.[1]

Interoperabilita neboli schopnost různých systémů vzájemně spolupracovat a poskytovat si služby, je důležitá mezi heterogenními a distribuovanými systémy. Aby bylo možné podporovat interoperabilitu v oblasti internetu věcí, je třeba standardizovat referenční model architektury internetu věcí.

Autonomní síť musí být dále podporována v síťových řídicích funkcích internetu věcí, aby se přizpůsobily různým aplikačním oblastem, různým komunikačním prostředím a velkým počtům a typům zařízení. Mezi typické aplikační domény patří průmysl, životní prostředí, společnost a domov. V průmyslu se jedná o činnosti spojené s finančními nebo obchodními transakcemi mezi společnostmi, organizacemi a jinými subjekty. Dalším příkladem je výroba, logistika, služby, bankovníctví a jiné. Ohledně životního prostředí jsou to aplikace týkající se ochrany, sledování a rozvoje všech přírodních zdrojů, jako je například recyklace a energetické řízení. Doména týkající se společnosti se zabývá rozvojem a začleňováním společností, měst a lidí. Mezi příklady patří například vládní služby směřující k občanům a veřejná doprava. V domácnosti se jedná o činnosti týkající se jednotlivců a rodinných příslušníků, kde příkladem může být sledování vlastního zdraví (hmotnost, spánek atd.).

Autonomní služby mohou záviset na technice automatické fúze dat a dolování dat. Služby musí být poskytovány automatickým zachycováním, komunikací a zpracováním dat o věcech na základě pravidel nakonfigurovaných operátory nebo přizpůsobených odběrateli. Autonomní služby jsou nutné k automatickému snímání, komunikaci a zpracování dat věcí.

Internet věcí podporuje lokalizační služby. Komunikace a služby týkající se něčeho závisí na informacích o poloze věcí a uživatelů. Je třeba, aby informace o poloze byly automaticky zjišťovány a sledovány. Místní komunikace a služby mohou být omezeny zákony a předpisy a měly by být v souladu

s bezpečnostními požadavky. Každá věc v rámci internetu věcí je spojena, což vede k významným bezpečnostním hrozbám, jako jsou ohrožení důvěrnosti, autenticity a integrity dat i služeb. S bezpečností také souvisí ochrana soukromých dat. Každá věc má svého vlastního majitele a uživatele. Zaznamenané údaje o věcech mohou obsahovat soukromé informace týkající se jejich vlastníků nebo uživatelů. Internet věcí musí podporovat ochranu soukromí při přenosu dat, agregaci, ukládání, těžbě a zpracování, ale zároveň by ochrana soukromí neměla bránit ověřování datového zdroje.[1]

Služby vztahující se k lidskému tělu se týkají služeb poskytovaných zachycováním, komunikací a zpracováním dat týkajících se statických vlastností člověka a dynamického chování s lidskou intervencí nebo bez ní. Různé země mají v těchto službách odlišné zákony a předpisy.

Pro zajištění normálních síťových operací je nutná ovladatelnost. Aplikace internetu věcí obvykle fungují automaticky bez účasti lidí, ale jejich celá operační procedura by měla být zvládnutelná příslušnými stranami.

Funkci plug-and-play je třeba podporovat v internetu věcí tak, aby umožňovala generování, sestavování nebo získávání sémantických konfigurací na bezproblémové integraci a spolupráci věcí s aplikacemi. Jde o konfigurování zařízení na bázi sémantiky. Plug-and-play se dělí na PnP funkce správy a PnP funkce zabezpečení. Co se týče funkce správy, jde o řízení, které zajišťuje správu chyb, správu konfigurace a aktivaci nebo deaktivaci plug-and-play. Při připojení zařízení k síti se zajistí schopnost správy a řízení, kde se pokusí získat vlastnosti zařízení, mezi které patří výrobce, model, aplikační protokol, paměťový prostor a další.[6]

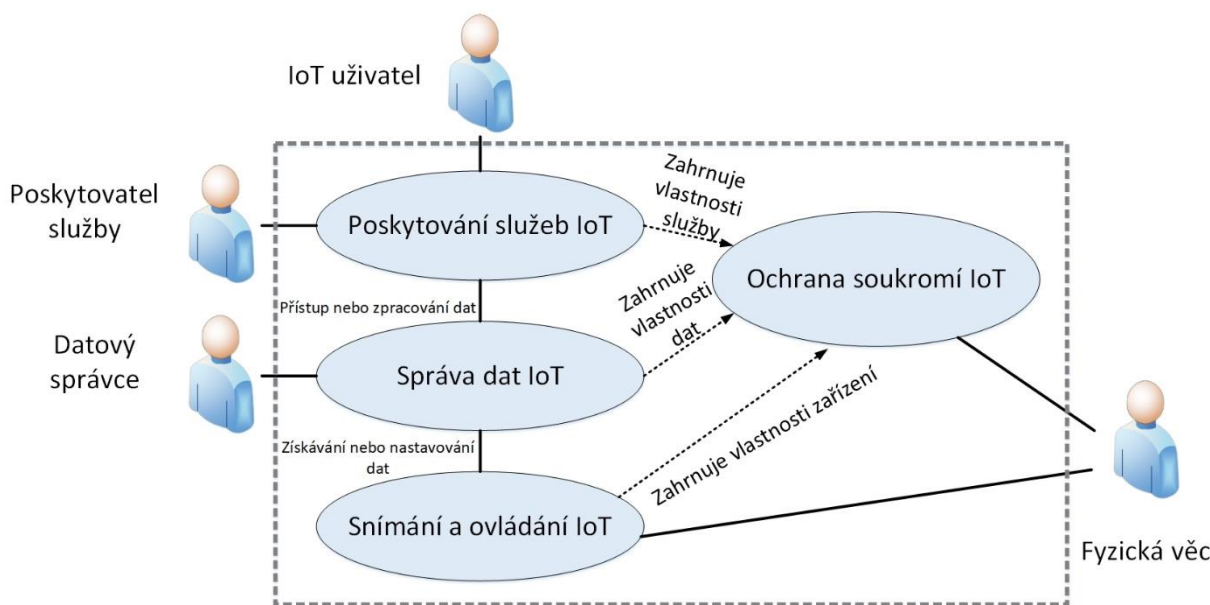
Úkol pro funkci zabezpečení je ověření a autorizace mezi přístrojem a internetem věcí, hned po tom o se zařízení připojí k síti. Zabezpečení může probíhat automaticky nebo manuálně. Manuální konfigurace je bezpečnější a nepotřebuje žádnou dodatečnou bezpečnostní ochranu. Při konfiguraci automatické může dojít k přeskočení některých základních bezpečnostních kroků, a to způsobí větší zranitelnost síťových útoků.

2.6 POUŽITÍ

Na obrázku můžeme vidět model obecného použití internetu věcí. Tento model se skládá ze čtyř obecných případů, mezi které patří snímání nebo ovládání internetu věcí, správa dat internetu věcí, poskytování služeb internetu věcí a ochrana soukromí internetu věcí.

Případy použití mohou být uplatněny k zachycení požadavků systému. Model použití může ukázat interakce mezi systémem a subjekty, které jsou mimo systém. Tyto externí subjekty v internetu věcí jsou označovány jako "IoT aktéři".[7]

Aktér internetu věcí je entita, která je mimo Internet věcí ale interaguje s ním. Každý případ použití zahrnuje funkční požadavky externích subjektů zapojených do použití. Externí subjekty rozdělujeme do čtyř skupin. První skupinou jsou fyzické věci, další je datový správce, poskytovatel služeb a poslední skupinou jsou sami uživatelé internetu věcí.



Obrázek 5 - Obecný případ využití Internetu věcí[8]

Fyzická věc je externí subjekt, který má ve fyzickém světě jedinečný identifikátor. Jejím úkolem je interakce s internetem věcí prostřednictvím snímání nebo ovládání činností. Fyzická věc se může dále rozdělit na umělou věc nebo přírodní věc. Umělá věc je fyzická věc, která je vyrobena pomocí lidského zásahu a může být označena sériovým číslem na produktu. Fyzická věc přírodní je generovaná přírodou a její značení je přiřazeno například podle času, místa nalezení nebo kategorií.[7]

Důležitá činnost je ochrana soukromí internetu věcí, což zahrnuje činnosti zabezpečení a skrytí soukromých informací o fyzických věcech. Ochrana soukromí je spjata se všemi ostatními souvisejícími úkoly, jako je snímání nebo ovládání, spravování dat a poskytování služeb.

Snímání nebo ovládání zahrnuje činnosti zabývající se konektivitou s fyzickými věcmi, zjišťování stavů fyzických věcí nebo samotné ovládání fyzických věcí.

Dalším externím subjektem je datový správce. Tento datový správce je také rozdělen do dvou skupin, a to lidský datový správce a mechanický datový správce, kde každý typ je použit při různém použití

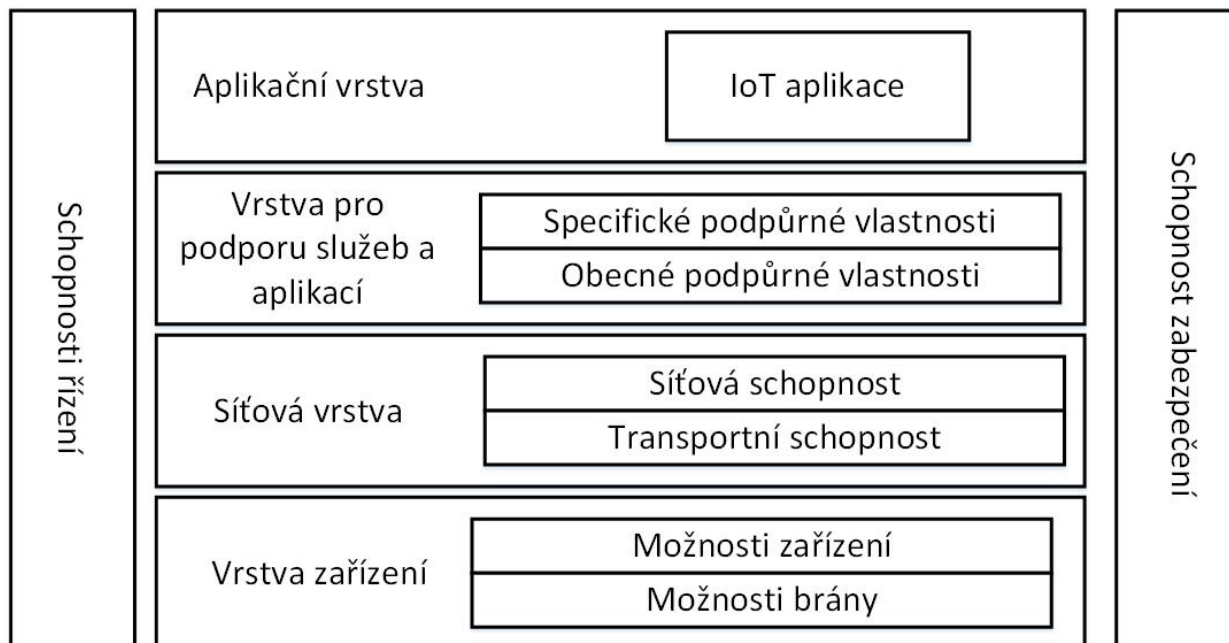
správy dat internetu věcí. Lidský datový správce provádí na internetu správu dat ručně, zatímco mechanický ji provádí automaticky. Hlavní činnost je spravování dat, což zahrnuje zachycování, ukládání, přenos a zpracování dat internetu věcí. Spravování dat souvisí s dvěma dalšími činnostmi, mezi které patří snímání nebo ovládání a provozování služeb.

Provozovatel služeb umožňuje monitorování, sledování polohy, zjišťování služeb a další služby související s internetem věcí. Mezi subrole poskytovatele služeb také patří poskytovatel aplikací, poskytovatel platformy a poskytovatel sítě. Jsou dva druhy provozovatele služeb. Prvním je společný poskytovatel takových služeb, které nejsou závislé na konkrétních aplikačních doménách. Druhý je aplikační poskytovatel služeb, který poskytuje aplikace založené na specifických aplikačních doménách. [7] Činnost poskytování služeb zahrnuje jak poskytování služeb provozovatelem, tak i využívání služeb uživatelem internetu věcí.

Poslední skupinou jsou uživatelé internetu věcí, to je skupina aktérů internetu věcí, která využívá všechny možné služby související s internetem věcí.

2.7 REFERENČNÍ MODEL INTERNETU VĚCÍ

Referenční model internetu věcí se skládá ze čtyř vrstev: aplikační vrstvy, vrstvy pro podporu služeb a aplikací, síťové vrstvy a vrstvy zařízení.



Obrázek 6 - Referenční model pro Internet věcí[2]

Aplikační vrstva obsahuje aplikace internetu věcí. Aplikace zahrnují různé druhy aplikací, např. inteligentní dopravní systémy, inteligentní síť nebo inteligentní domov. Aplikace mohou být založeny na proprietárních aplikačních platformách, ale mohou být také postaveny na společné platformě podpory služeb, které poskytují obecné možnosti, jako je autentizace, správa zařízení, nabíjení a účtování.

Vrstva pro podporu služeb a aplikací se skládá ze dvou skupin schopností, specifické podpůrné schopnosti a obecné podpůrné schopnosti. Obecné podpůrné schopnosti jsou společné funkce, které mohou být použity v různých aplikacích internetu věcí, jako je zpracování dat nebo ukládání dat. Tyto schopnosti mohou být také vyvolány specifickými podpůrnými schopnostmi, například k vytvoření dalších specifických možností podpory. Specifické podpůrné schopnosti jsou specifické schopnosti, které vyhovují požadavkům různorodých aplikací. Ve skutečnosti se mohou skládat z různých detailních seskupení schopností s cílem poskytovat různé podpůrné funkce různým aplikacím internetu věcí.

Síťová vrstva má také dvě skupiny schopností, síťovou schopnost a transportní schopnost. Síťová schopnost poskytuje příslušné řídicí funkce připojení k síti, jako jsou funkce kontroly přístupu a dopravy, řízení mobility nebo ověřování, povolení a účetnictví. Transportní schopnost je schopnost soustředit se na poskytování připojení k přenosu informací o službách internetu věcí a specifických aplikačních informacích.

Možnosti zařízení a možnosti brány tvoří vrstvu zařízení. V přímé interakci s komunikační sítí jsou zařízení schopna shromažďovat a odesílat informace přímo, to znamená bez použití funkcí brány, do komunikační sítě a mohou přímo přijímat informace z komunikační sítě. V nepřímé interakci s komunikační sítí jsou zařízení schopna shromažďovat a odesílat informace do komunikační sítě nepřímo, tj. prostřednictvím funkcí brány. Na druhé straně zařízení mohou nepřímo přijímat informace z komunikační sítě. Při síťovém připojení ad-hoc mohou zařízení vytvářet sítě ad-hoc způsoby, které vyžadují větší škálovatelnost a rychlé nasazení. [1]

Možnosti zařízení mohou podporovat mechanismy spánku a probuzení, které šetří energii. V možnostech brány je podpora více rozhraní a konverze protokolů. Při podpoře více rozhraní dochází na vrstvě zařízení k podpoře funkce brány zařízení připojené prostřednictvím různých druhů drátových nebo bezdrátových technologií. Příklady těchto technologií jsou například sběrnice CAN, ZigBee, Bluetooth nebo Wi-Fi. V síťové vrstvě mohou být brány schopny komunikovat prostřednictvím různých technologií, jako jsou veřejná telefonní síť (PSTN), síť druhé generace nebo třetí generace (2G nebo 3G), technologie určená pro vysokorychlostní internet v mobilních sítích (LTE), ethernet nebo technologie využívající stávající vedení telefonu nebo kabelové televize pro vysokorychlostní přenos dat (DSL).

V konverzi protokolů existují dvě situace, kdy jsou zapotřebí možnosti brány. První situace spočívá v tom, že komunikace na vrstvě zařízení používají různé protokoly vrstvy zařízení, například protokoly technologie ZigBee a protokoly technologie Bluetooth. Druhá situace je, když komunikace zahrnující vrstvu zařízení i síťovou vrstvu používají různé protokoly, jako například protokol ZigBee technologie na vrstvu zařízení a protokolu technologie 3G na síťové vrstvě.

Schopnosti řízení podobně jako tradiční komunikační sítě pokrývají schopnosti správy internetu věcí tradiční třídy poruch, konfigurace, účetnictví, výkonu a zabezpečení. Možnosti řízení internetu věcí lze rozdělit do obecných schopností správy a specifických manažerských schopností. K základním funkcím obecného řízení patří, řízení topologie místní sítě, správa zařízení a řízení provozu a přetížení. Správa zařízení je například aktivace a deaktivace vzdáleného zařízení, diagnostika, aktualizace softwaru a řízení stavu zařízení.[1]

Řízení provozu a přetížení je například zjišťování podmínek přetečení sítě a provádění rezervace zdrojů pro časově kritické a životně důležité datové toky.

Existují dva druhy bezpečnostních funkcí, obecné bezpečnostní schopnosti a specifická bezpečnost. Specifické bezpečnostní funkce jsou úzce propojeny s konkrétními požadavky pro konkrétní aplikace, jako jsou mobilní platby a bezpečnostní požadavky. Generické bezpečnostní funkce jsou nezávislé na aplikacích a obsahují určité funkce na daných vrstvách. Na aplikační vrstvě je to oprávnění, ověřování, důvěrnost údajů a ochrana integrity, ochrana soukromí, bezpečnostní audit a antivirus. Na vrstvě síťové to je oprávnění, ověřování, utajení důvěrných dat a signalizačních dat a ochrana celistvosti signalizace a na vrstvě zařízení je autentizace, autorizace, validace integrity zařízení, kontrola přístupu, důvěrnost údajů a ochrana integrity.

3 M2M

Technologie M2M neboli komunikace mezi stroji je klíčovým nástrojem k internetu věcí. Z předchozích definic internetu věcí je zřejmé, že se jedná o vzdálený přístup k zařízení. Na stejném principu funguje samozřejmě i M2M komunikace. Pro Internet věcí jsou základní jednotkou věci, jak fyzické, tak virtuální. V komunikaci M2M se jedná o přímou komunikaci strojů mezi sebou. Pro Internet věcí je důležitý IP protokol, který umožní propojení dat zařízení s cloudovou platformou. Na rozdíl od toho komunikace M2M využívá přímou komunikaci typu point-to-point neboli bodová řešení.[9] Bodové řešení se v M2M aplikacích obvykle skládají z hardwarových modulů zabudovaných do počítače v místě zákazníka, které komunikují skrze mobilní sítě se softwarovými aplikacemi, nejčastěji u dodavatele.[10]



Obrázek 7 - Porovnání M2M a IoT[11]

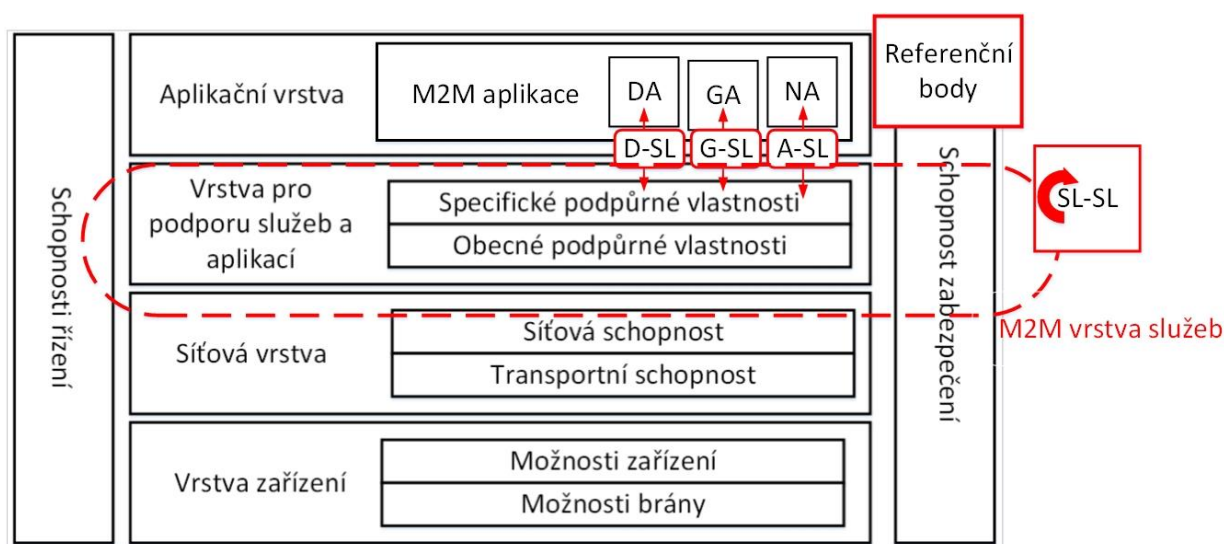
3.1 M2M REFERENČNÍ MODEL

Stejně jako u internetu věcí má referenční model čtyři základní vrstvy. Všechny vrstvy, kromě vrstvy aplikační jsou identické s vrstvami pro Internet věcí. Aplikační vrstva obsahuje místo aplikací internetu věcí, M2M aplikace. Ve vrstvě aplikační jsou identifikovány tři typy aplikací.

Jedná se o aplikace:

- zařízení (DA = device application)
- brány (GA = gate application)
- síťové (NA = network application)

Všechny tyto tři aplikace jsou v zařízení, bráně a síťovém aplikačním serveru a mohou využívat schopnosti M2M.[12]



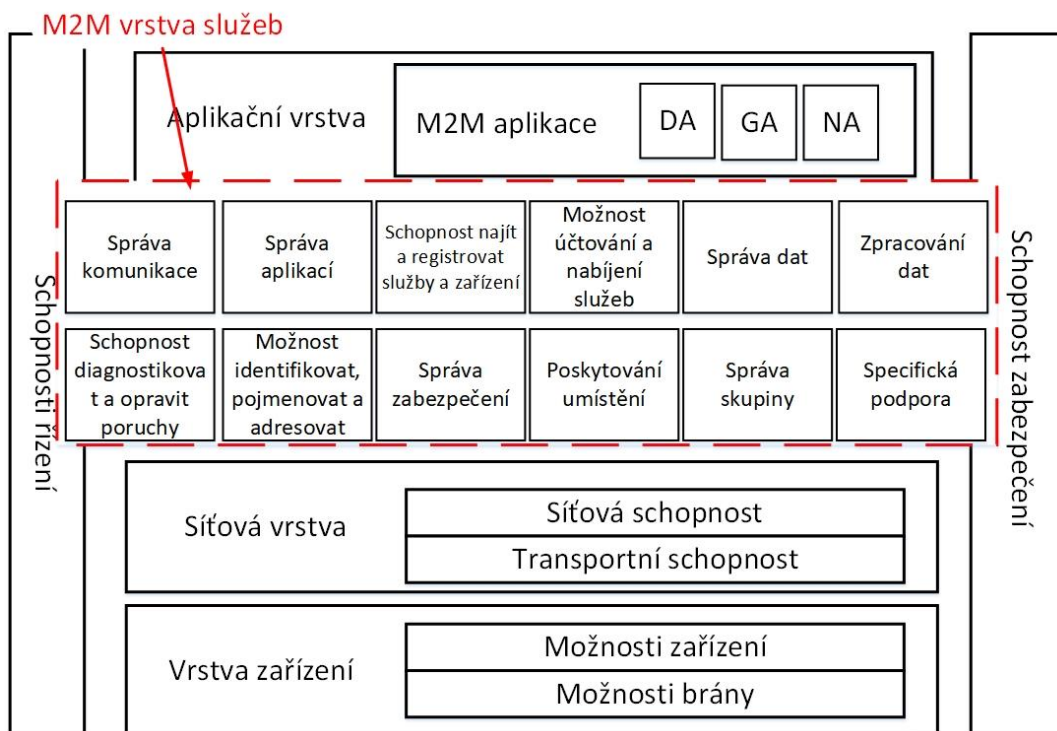
Obrázek 8 - Referenční model M2M a vyobrazení referenčních bodů[13]

Platforma M2M je součástí síťového aplikačního serveru a je považována za skupinu technologií, která se používá jako základ, na kterém jsou aplikace, procesy či jiné technologie vyvíjeny nebo dodávány.

Platforma zahrnuje mnoho platformových funkcí. První funkce je podpora připojení, která zahrnuje všechny možné důležité úkoly, které je třeba provést při konfiguraci a podpoře připojení M2M. Například v mobilním prostředí podpora připojení zahrnuje zajištění připojení, využití monitorování a určitou úroveň podpory pro řešení poruch. Další je povolení služby, která má mnoho možností v rámci podpory řešení, oznamování a poskytování softwarového prostředí. Pro usnadnění prodeje zařízení potřebujeme platformu, která má funkci správy zařízení. Správa zařízení se dá srovnat s výrobcí jednotlivých zařízení a podporuje zařízení různých druhů.[12]

Podpora aplikací zahrnuje konektivitu více typů zařízení, konektivitu s několika technologiemi a konektivitu sítí s několika poskytovateli komunikačních služeb. Poslední funkce platformy je poskytovatel řešení. Tento druh platformy je obecně využíván systémovými integrátoři neboli firmami zajišťujícími komplexní realizaci spojování softwarových komponent subsystému.

3.2 ARCHITEKTONICKÝ RÁMEC VRSTVY M2M



Obrázek 9 - Architektonický rámec v M2M vrstvě služeb[13]

M2M servisní vrstva má několik důležitých schopností, které je třeba definovat pro komunikaci mezi stroji.

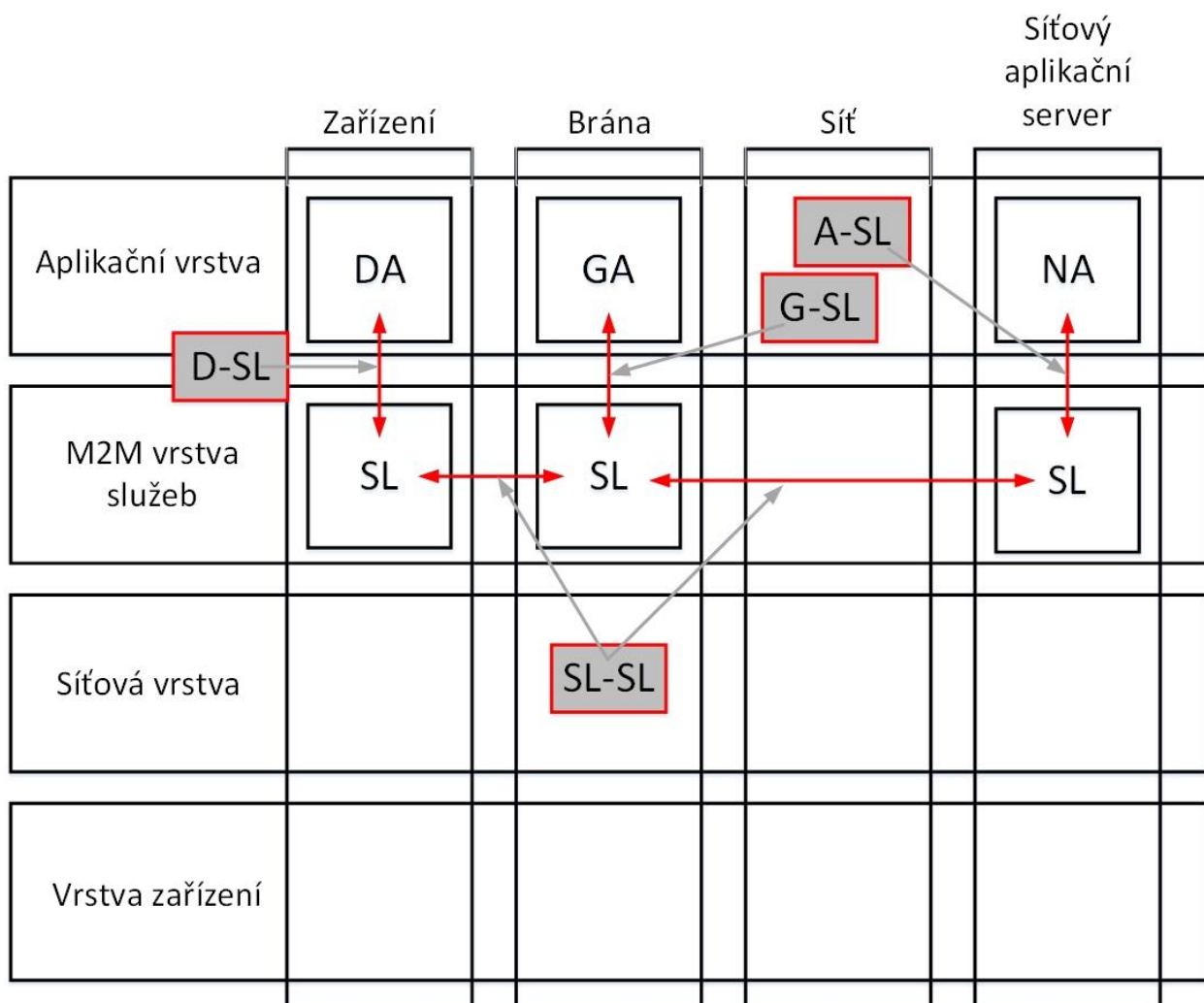
- Správa komunikace podporuje plánování zpráv, různé typy komunikací a různé síťové technologie. Mezi typy komunikace patří například: nepřetržitá, na požádání nebo oznámení o selhání.
- Správa aplikací vyžaduje podporu více aplikací fungujících současně.
- Najít a registrovat služby nebo zařízení je další schopnost vrstvy M2M.
- Účtování a nabíjení služeb se dá realizovat nabíjením off-line nebo online.
- Správa zařízení je funkce, která podporuje automatickou konfiguraci několika zařízení a několika typů zařízení.
- Funkce zpracování dat se skládá z ukládání dat, oznamování, formátování, překlad, sběr a report.
- Diagnostika a opravení poruchy je další schopností vrstvy, kde dochází k rozpoznání poruchy a její izolace, dále její opravy a protokolování.
- Další funkcí je identifikace, pojmenování a adresování při dostupnosti zařízení.
- Zabezpečení je důležitá funkce, která podporuje autentizaci, ochranu soukromí a důvěrnost.
- Poskytování umístění je založeno na získávání informací o poloze a jejich správě.
- Správa skupiny je mechanismus založený na vytváření a řízení virtuální skupiny zařízení.
- Specifická podpora se vztahuje ke konkrétním aplikacím.[12]

3.3 REFERENČNÍ BODY

Bodové řešení je druh komunikace využívaný v M2M. Mohou nastat čtyři různé situace odvíjející se mezi jakými body dojde k vytvoření spojení. Referenční body jsou použity na servisní vrstvě jak pro obecné podpůrné schopnosti, tak i pro specifické podpůrné schopnosti.

Prvním druhem je D-SL, jedná se o referenční bod mezi zařízením (D) a servisní vrstvou (SL). G-SL je referenční bod mezi bránou (G) a servisní vrstvou. Dalším druhem je NA-SL, kde se jedná o referenční bod mezi síťovou aplikací (NA) a servisní vrstvou. A posledním příkladem referenčního bodu je takový druh bodu, který je mezi různými servisními vrstvami.[14]

Příklad využití referenčních bodů v praxi je například aplikační programovací rozhraní nebo protokoly.



Obrázek 10 - Referenční body v referenčním modelu M2M[13]

4 API A PROTOKOLY

API je zkratka pro Application Programming Interface, což je aplikační programovací rozhraní. Toto rozhraní obsahuje sadu příkazů, rutin, funkcí, nástrojů a protokol pro vytváření aplikací. Rozhraní API umožní používat předem nadefinované funkce pro interakci s operačním systémem. Úkolem aplikačního rozhraní je ochrana aplikací od základních zdrojů a omezuje úsilí spojené s rozvojem služeb. Standardizované rozhraní má za cíl zajistit efektivitu a interoperabilitu služeb. Mnoho společností začalo vystavovat aplikační programovací rozhraní v kontextu M2M.

Protokol je sada pravidel umožňující propojování a přenášení dat mezi dvěma zařízeními. Mezi klíčové funkce protokolu patří zobrazení dokončení zprávy u odesílacího zařízení, zobrazení přijetí zprávy u přijímacího zařízení a typ kontroly chyb, který je použit pro kompresi dat.

V M2M komunikaci existuje již několik aplikačních rozhraní a protokolů, jako je NAT-PMP, DPWS, SOAP, OAuth, WebSocket.

NAT-PMP je protokol mapování portů, který slouží pro automatizaci procesu vytváření mapování překladů síťových adres. Umožňuje počítači, který je v soukromé síti nakonfigurovat směrovač automaticky. V podstatě automatizuje proces předávání portů. V protokolu je zahrnut způsob získávání veřejné IP adresy. Zařízení pro službu webových služeb neboli DPWS, definuje minimální sadu omezení, která umožňují zasílání zpráv, zjišťování a popis zařízení s omezeným přístupem. Služba DPWS obsahuje rozšíření, které umožní bezproblémovou integraci.

Jednoduchý objektový přístupový protokol SOAP je lehký protokol určen pro výměnu informací, které jsou strukturované v decentralizovaném a distribuovaném prostředí.

Autorizační rámec OAuth 2.0 umožňuje aplikaci třetí strany získat omezený přístup k službě HTTP buď jménem vlastníka zdroje tím, že uspořádá interakci o schválení mezi vlastníkem zdroje a službou HTTP nebo tím, že umožní třetímu účastníkovi získat přístup.

Protokol WebSocket je bezpečnostní model, který běžně používá webový prohlížeč a umožňuje obousměrnou komunikaci mezi klienty, kteří pracují s nedůvěryhodným kódem.[14]

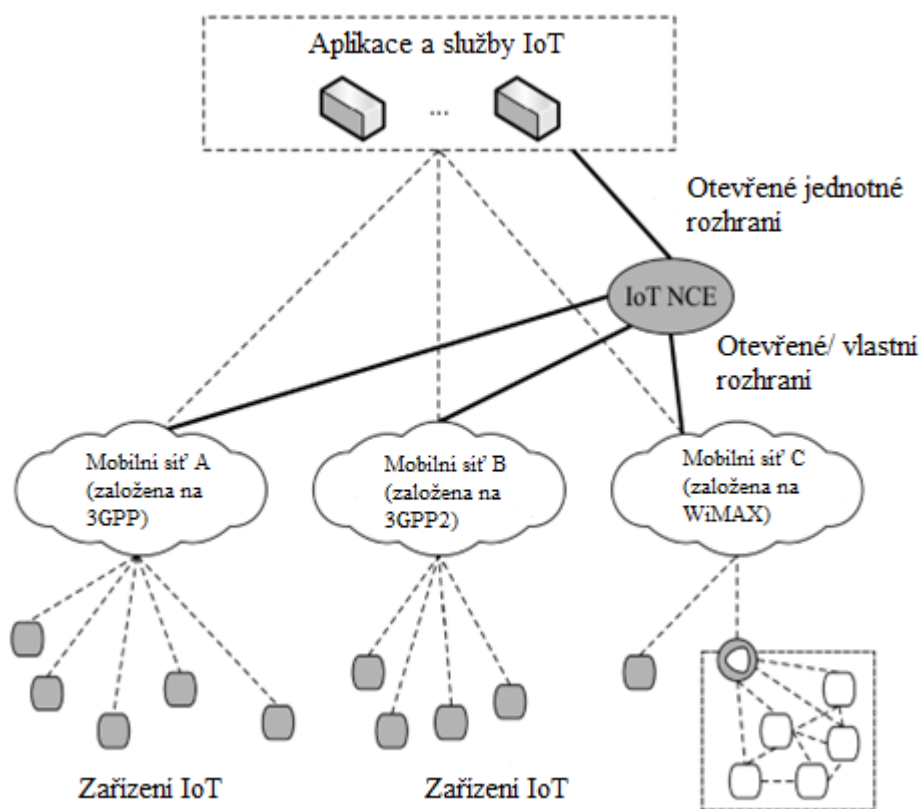
4.1 VYUŽITÍ API

Aplikační programovací rozhraní je důležité pro IoT NCE (Network Capability Exposure). NCE Internet věcí je jednotka, která usnadňuje službám, zařízením a daným aplikacím internetu věcí plně využívat základní síť a jejich různě síťové schopnosti. NCE umožňuje přístup pro poskytovatele sítí na různé proprietární platformy, kde může spravovat zařízení internetu věcí nebo řídit dynamicky komunikaci. Mezi základní sítě patří 3GPP, 3GPP2 a WiMAX.[15]

3GPP síť je založena na technologii pro komunikaci, mezi které patří GSM – Globální systém pro mobilní komunikaci, jeho nástupce LTE – dlouhodobý vývoj pro vysokorychlostní Internet v mobilních sítích, WCDMA – širokopásmový vícenásobný přístup s kódovým dělením a NB IoT – úzkopásmový přístup pro Internet věcí.

3GPP2 je síť komunikačních standardů založena především na kódovém multiplexu.

Mezi další síť založenou na sérii komunikačních standardů patří WiMAX. WiMAX je bezdrátová technologie s mikrovlnným připojením, která je stále ve vývoji.



Obrázek 11 - Přehled síťových využití pro Internet věcí[16]

Na obrázku můžeme vidět dva druhy interakce. První interakce, která je vyznačena silnější čarou, je interakce probíhající mezi IoT NCE a mobilními sítěmi, nebo mezi IoT NCE a aplikacemi nebo službami IoT. Čárkovane vyznačená interakce označuje komunikaci mezi sítěmi, IoT aplikacemi a službami a IoT zařízeními.

5 TELEKOMUNIKAČNÍ SÍTĚ

Internet věci v některých případech potřebuje pro svoji práci síť s širokým pokrytím. Takovým příkladem jsou například mobilní sítě. Mobilní sítě již pokrývají 90 % světové populace a jsou postaveny tak, aby zvládly masivní objemy mobilního širokopásmového provozu. Mobilní síť se řídí fórem pro standardizaci 3GPP.

5.1 MOBILNÍ SÍŤ A 3GPP

Veřejné mobilní sítě můžeme rozdělit do několika generací podle jejich vlastností. 3GPP je zkratka pro partnerský projekt třetí generace, který začal vytvářet standardy pro síť třetí generace (3G) neboli UMTS (Universal Mobile Telecommunication System). Systémy pracují ve frekvenčním pásmu o velikosti 2 GHz. Třetí generace na rozdíl od těch předchozích nabízí infrastrukturu s garantováním přenosu multimédií s danou kvalitou. Samozřejmě obsahuje IP protokol s přímým připojením do internetu. Připojení do internetu je již možné od rozšířené druhé generace. Hlas je v síti přenášen digitálně již od druhé generace. Dnes už však vyvíjí sítě vyšších generací, jako je 4G a 5G.[17]

První fáze projektu začala 1.1.1987, avšak až v roce 1999, vyšlo první zveřejnění standardu základních specifikací GSM a UTRAN, rádiové přístupové sítě. Od Release z roku 1999 k Release 7 došlo k mnoha vývojovým pokrokům, jako je například zavedení VoIP (přenos hlasu pomocí IP protokolu, které se používá zejména pro telefonování za využití internetu), operace s LAN sítí, zpracování soukromých dat, mnoho pokroků nastalo také v oblasti MMS a dalších sektorech.

Pro využití v M2M komunikaci je pro nás nejdůležitější fáze týkající se LTE a NarrowBand IoT. První zmínky o LTE mobilním internetu jsou v Release 8, kde jsou nastaveny určité vyšší požadavky pro internetovou síť. Mezi požadavky patří snížení ceny za bit, více služeb, flexibilita používání frekvenčních pásem a zjednodušená architektura.[18]

Od Release 9 dochází stále ke zdokonalování služby LTE, zejména v oblasti frekvenčního pásma. V Release 11 došlo k propojení mezi operátory na služební vrstvě. Také došlo k zvýšení horního pásma na 850 MHz. Většina operátorů na světě používá pásmo 800 MHz. Prioritou v Release 12 bylo využití technologie LTE pro nouzové a bezpečnostní služby s technickými specifikacemi pro kritické funkce aplikační vrstvy. Do zatím poslední fáze se dostal Release 13, který se zabývá specifikací NarrowBand IoT a specifikacemi kritických služeb. Začala se řešit virtualizace sítí a jejich realizace v 3GPP síti. Na Release 14 se pracuje v tomto roce 2018.

5.2 ROZSÁHLÁ SÍŤ S NÍZKOU SPOTŘEBOU

Pro připojení zařízení IoT, která vyžadují obrovské množství výměny dat, je potřeba různých systémů a technologií. Technologie, která je velice vhodná pro aplikace internetu věcí nebo M2M komunikace je LPWA. Low-Power Wide-Area, to jsou sítě pro rozsáhlé území s nízkenergetickým standardem. Systémy LPWA jsou navrženy tak, aby odpovídaly požadavkům pro širokou oblast a zároveň pro nízkou spotřebu. Všechny sítě s tímto přístupem musí mít pokrytí zvýšené o 15-20 dB oproti GSM a LTE. Sítě LPWA jsou určeny pro aplikace typu IoT a M2M, které mají nízké přenosové rychlosti, dlouhou životnost baterie, optimalizované náklady a fungují i ve vzdálených a těžko dostupných místech. Rozsáhlé sítě s nízkou spotřebou můžeme rozdělit na dvě základní skupiny, podle licencování. Sítě mohou být buď licencované nebo nelicencované.[19]

5.2.1 LICENCOVANÉ LPWAN

Licencovaná rozsáhlá síť s nízkou spotřebou může být považována za synonymum pro síť mobilní, protože jsou navrženy tak, aby byly integrovány do stávajících buněčných infrastruktur. Nejen, že jsou považovány jako mobilní sítě, ale jsou také standardizovány dle 3GPP v předposlední Release neboli v poslední dokončeném Release 13. Do kategorie licencovaných rozsáhlých sítí se tak řadí LTE-M, EC-GSM, NB-IoT a LTE 450.[20]

LTE-M je vysokorychlostní internet určen pro „Machine“ komunikaci. LTE-M podporuje bezpečnou komunikaci, vysokou kapacitu systému, všudypřítomné pokrytí a je navrženo tak, aby se snížila složitost zařízení. LTE-M je plně duplexní systém, který umožňuje oboustranné duplexní dělení, poloduplexní dělení a duplexní časové dělení. Tím, že působí jako plně duplexní systém na větší šířce pásma, dokáže nabídnout služby s nižší latencí a vyšší propustností než NarrowBand IoT a EC-GSM.[21]

Extended Coverage GSM IoT, je rozšířené pokrytí GSM sítě pro Internet věcí a vychází z GPRS sítě. General Packet Radio Servis je služba pro přenos dat a pro připojení na internet pro mobilní telefony, umožňující komunikaci v pásmech 850, 900, 1800 a 1900 MHz, které podporují roaming ve většině částech světa. V EC-GSM je v porovnání GPRS lepší pokrytí o 20 dB, bezpečnostní stupeň LTE a energeticky úsporný provoz.[21]

LTE 450 využívá pásmo 450 MHz. Nyní je 450 MHz využíváno pro CDMA, kódový multiplex, ale O2 přemýšlí o využití tohoto pásma pro přenos LTE. Tento přenos LTE by sloužil pro M2M zařízení. Oproti NB IoT má výhodu v tom, že nepotřebuje vybudovat tolik základnových stanic pro pokrytí celého území. Výhodou v pásmu 450 MHz je nižší frekvence, tudíž delší dosah a lepší pokrytí. LTE 450 je zatím jen plánové a dnes O2 využívá na M2M komunikaci buďto jen GSM síť, pro případy, kdy se nemusí přenášet žádná data. Bez dat tudíž můžeme ovládat topení, zavlažování, otevírání vrat a jiné, pouze pomocí zaslání SMS nebo prozvonění. Pro přenos dat se používá GPRS síť a slouží nám k sledování pohybu auta či sledování skrz kameru domu.

NarrowBand IoT neboli úzkopásmová bezdrátová technologie využívaná pro Internet věcí je síť pro rozsáhlé území. Technologie je úzkopásmová, protože šířka pásma je pouze 200 kHz. Jedná se o velice nízkoenergetický standard s nízkými náklady, nízkou spotřebou a optimalizovanou síťovou architekturou.[22] NarrowBand IoT je novou technologií rádiového přístupu na rozdíl od LTE a EC-GSM, které jsou založeny na stávajících technologiích rádiového přístupu. Podporuje minimální šířku pásma kanálu, která je pouze 3,75 kHz, a to umožní nesrovnatelnou flexibilitu spektra a kapacitu systému. NarrowBand IoT je navrženo pro takové aplikace, které komunikují s velkým množstvím dat po dlouhou dobu. Zdá se, že nevýhodou je přenosová rychlost, která je v kB/s, ale to pro M2M aplikace to stačí. První modul pro NarrowBand IoT vyrobila firma Ublox. Jedná se o SARA-N2 modul s nízkou spotřebou energie, kde životnost může být až 10 let. Modul má mnoho výhod, jako je velký teplotní rozsah od -40 do 85 stupňů, velký dosah, snadná migrace mezi ostatními moduly ublox a malá velikost.[23] Firma Ublox také vyrábí kity neboli vyhodnocovací sady pro mobilní moduly NarrowBand IoT s jednoduchým přístupem, snadným testováním a rozsáhlou vizualizací. Sady se používají přes USB rozhraní a vyžadují aktivní SIM kartu. [24] Narrowband IoT je v České Republice zatím podporován pouze operátorem Vodafone. O2 pracuje na vývoji jak NB IoT, tak ale také na LTE 450.

5.2.2 NELICENCOVANÉ LPWAN

Opakem mobilních sítí s masivním přístupem jsou nelicencované nízkoenergetické širokopásmové sítě, již jsou poskytovány firmami například SigFox a LoRaWAN.

Prvním příkladem rozsáhle sítě s nízkou spotřebou, která je rozmístěna v nelicencovaném pásmu je technologie SigFox. Tato technologie využívá ultra úzké pásmo, pouze 192 kHz a typická propustnost je 100 nebo 600 b/s. Úzkopásmová síť má nižší vstupní šum v pásmu a tím může mít více kanálu než širokopásmová síť. SigFox je technologie, která není navržena pro přenos velkého množství dat. Zařízení obvykle posílají 140 zpráv denně. Každá zpráva je o šířce 100 Hz, velikosti 0-12 byte a pošle se vždy třikrát pokaždé na jiné frekvenci, aby bylo zaručeno doručení. Příklady takto malých zpráv jsou například zprávy o poloze pomocí GPS, která má 6 bajtů, o teplotě má 2 bajty a o rychlosti mají pouze jeden.[25] SigFox je francouzská společnost s pokrytím komerčních sítí v přibližně 25 zemích, včetně zemí v Evropě a USA. Má i své partnerské operátory pro Českou Republiku a tím je SimpleCell Networks. SimpleCell Networks je první mobilní operátor pro Internet věcí. Pokrývá 95 % populace ČR a 92 % území ČR. Více než 80 firem se podílí na vyvíjení hardwaru a je více než 100 projektů s technologií SigFox v ČR. [26]

Další technologii pracující v nelicencovaném pásmu, kde spektrum je menší jak 1 GHz je technologie LoRa, která používá protokol LoRaWAN. LoRa má rozšířené spektrum, které může být rychleji nasyceno a tím může mít více problému s rušením v hustém prostředí. V digitální komunikaci je spektrální rozptyl spektra technikou využívající lineárně kmitočtově modulované kmity pulzů pro kódování informací. Protokol LoRaWAN je založený na modulační technologii. U firmy LoRa propustnost závisí na šířce pásma a může být 240 až 37500 b/s. Využívaná šířka pásma je 62,5 kHz, 125 kHz, 250 kHz a 500 kHz. [27] V Evropě má LoRa tři kanály o 125 kHz. Výchozí kanály jsou 868,10 MHz, 868,30 MHz a 868.50 MHz.

6 TRH

Podle ukazatele trhu mobilních sítí z otevřených dat Českého telekomunikačního úřadu ze dne 30.8.2017 můžeme vyčíst hodnoty týkající se SIM karet, hlasových služeb v pevné či mobilní síti, internetu v pevné síti a pro nás nejzajímavější M2M SIM karty. Samozřejmě jsou další odvětví týkající se trhu a počtu provolaných minut, ale to jsou data, která se netýkají Machine-to-Machine.

Tabulka 1 - Počet SIM dle ČTÚ

	2009	2010	2011	2012	2013	2014	2015	2016
SIM(mimo M2M)	13 075	12 934	13 168	13 330	13 105	13 226	13 273	13 370
M2M SIM	106	179	323	533	614	688	744	929

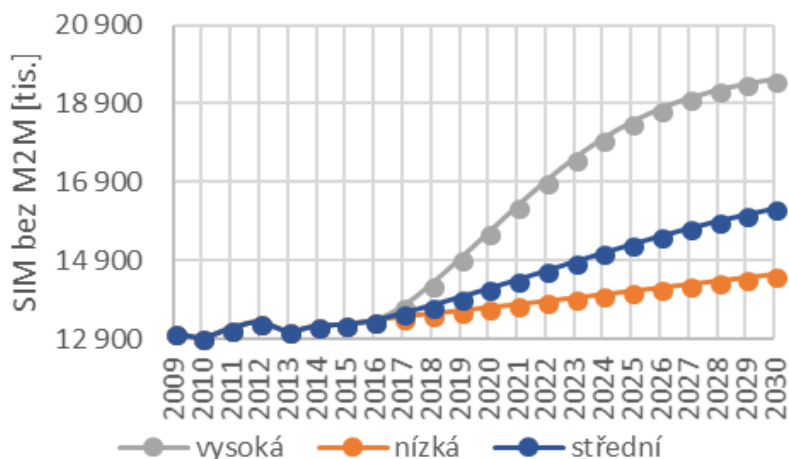
SIM karty můžeme rozdělit na aktivní SIM karty a M2M SIM karty. Aktivní SIM karty můžeme dále rozdělit na SIM karty post-paid a pre-paid. Kde post-paid jsou paušální tarify a pre-paid jsou předplacené karty. Machine-to-Machine karty nemají přesně definované rozdělení do skupin. Každý operátor člení M2M SIM karty dle různých použití. Podle firmy IBM hlavní odvětví M2M je sledování pohybu firemních vozidel, autonomní auta, sledování aktiv, monitorování energetiky, bankovníctví a sledovací zařízení. Český operátor O2 nabízí tarify podle množství dat, která přeneseme při používání M2M a jako své příklady uvádí sledování pohybu služebních aut, sledování mazlíčků a ovládání vrat. T-Mobile rozděluje M2M aplikace na sledování pohybu firemních vozidel, dohledová zařízení a zabezpečení objektů. Vodafone na svých stránkách zveřejňuje použití v sledování aut a bezpečnostních systémech. Operátor Nisatel nabízí pro Českou republiku M2M tarify, kde jako využití uvádí monitorování tepla, zabezpečení domů, bytů, garáží a chat. Pro lepší představu jsem seznam obohatila o zahraničního operátora, kde InfoSIM má své podkategorie monitorování energie, platební terminály, autonomní auta, monitorování zdraví a zabezpečení domů. Podle Berg Insight je na trhu M2M již rozšíření i v oblasti zemědělství, přesněji systémy v zemědělských strojích pracující na bázi M2M. Z těchto všech nabídek jsem sestavila rozdělení podle nejčastěji se opakujících využití, a tak jsem M2M rozdělila na sledování pohybu firemních aut, Smart Metering neboli měření energetiky, zabezpečení objektů, autonomní auta, zemědělství a zbytek jsou ostatní. Čísla jsou čerpána ze všech stávajících síťových operátorů, kterými jsou O2 Czech Republic a.s., T-Mobile Czech Republic a.s. a Vodafone Czech Republic a.s.

6.1 PREDIKCE TRHU

Všechny následující grafy sloužící pro predikci trhu obsahují tři různé křivky. Kde šedá křivka značí nejrychlejší nárůst SIM, oranžová nejpomalejší nárůst a modrá má růst střední. U predikce trhu pro Machine-to-Machine komunikaci je předpoklad, že nárůst bude ve tvaru tangens hyperbolický, to je tvar kdy v daném období dojde k velkému nárůstu počtu a po nějaké době se hodnoty ustálí. Všechny konkrétní hodnoty pro daný rok a danou skupinu nalezneme v příloze.

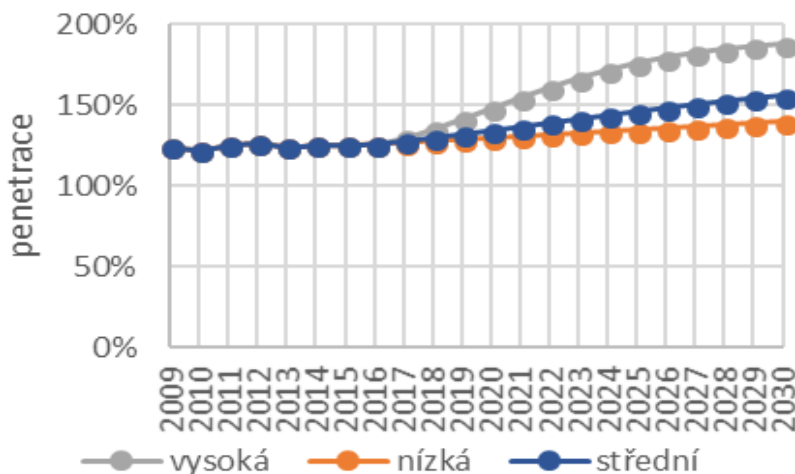
6.1.1 AKTIVNÍ SIM

Aktivní SIM, kde nejsou zahrnuty M2M SIM nejsou přímou náplní mé práce, ale je vhodné je zde zahrnout z hlediska porovnání a orientace. Hodnoty od roku 2009 do roku 2016 jsou čerpány ze statistik, podle regulátora České Republiky pro telekomunikační služby.



Graf 1 - Predikce počtu SIM bez M2M

Předpoklad počtu SIM karet při maximálním nárůstu dosahuje 19,5 milionům SIM karet, což je 188 % v roce 2030. Při minimálním nárůstu se dostaneme na hodnotu 14,5 milionu SIM karet a tím pádem penetrace je okolo 140 %.[28]



Graf 2 - Penetrace aktivních SIM karet

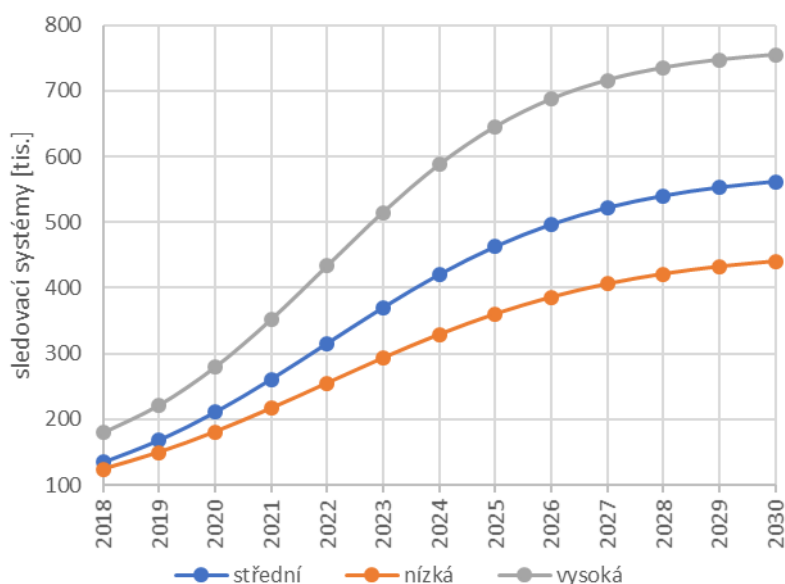
6.1.2 M2M

6.1.2.1 SLEDOVÁNÍ POHYBU FIREMNÍCH VOZIDEL

První odvětví, s využitím M2M, je sledování pohybu firemních vozidel neboli fleet management. Počítače palubních vozidel se poprvé objevili v 80. letech a brzy byly propojeny s různými satelitními a pozemními bezdrátovými sítěmi. V současné době mohou mobilní sítě v mnoha oblastech poskytovat všestrannou dostupnost připojení k internetu. Fleet Management využívá protokolování dat, satelitní polohu a datovou komunikaci, které umožňují správu vozidel a správu dopravy. Všechny tyto komponenty propojují vozidla a podnikové IT systémy.

V roce 2012 bylo v Evropské unii 3,05 milionu aut využívající fleet management. V roce 2017 se číslo sledovaných automobilů dokonce vyšplhalo až na 6,4 milionu. [29]

Predikované hodnoty pro systémy v automobilových vozech pro sledování pohybu jsou dále predikovány pro Evropskou unii a v roce 2021 by počet systémů měl být 14,1 milionů.[30]



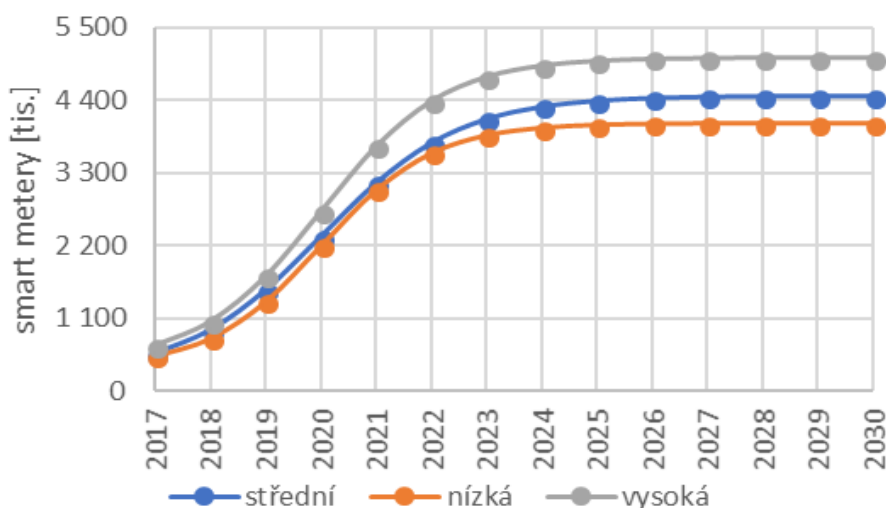
Graf 3 - Predikce počtu M2M SIM pro sledovací systémy

Počet 3,05 milionů vozidel využívající fleet management byl v roce 2012 0,85 % všech vozidel registrovaných v Evropské Unii, což je 357 milionů vozidel. V České Republice bychom ze všech 5,4 milionů registrovaných vozidel měli v roce 2012 vozidel se sledovacím systémem přibližně 46 tisíc. S hodnotou 14,1 milionu vozidel se sledováním pohybu dosáhne necelých 4 % všech registrovaných vozidel v Evropské Unii v roce 2021. Pokud by to platilo i pro Českou republiku, tak v roce 2021 budou 4 % všech vozidel vozidla využívat fleet management což bude představovat okolo 260 tisíc a v roce 2030 až 800 tisíc vozidel. Další hodnoty týkající se predikce trhu v oblasti sledovacích systémů u služebních aut najdete v příloze, tabulka 1 – Predikce počtu M2M SIM karet pro Fleet Management.

6.1.2.2 INTELIGENTNÍ MĚŘIČ

Další využití M2M je pro Smart Meter neboli inteligentní měřič, ten je jedním z hlavních složek inteligentních sítí Smart Grids. Kromě dat týkající se spotřeby energie nebo plynu také monitorují svůj vlastní výkon a prostředí. Inteligentní síť je zapojena do celé energetické sítě a související infrastruktury. Inteligentní sítě také pokrývají všechny aspekty elektrického toku, jako je výroba, dodávka, řízení a spotřeba. Datová komunikace je poskytována přes vnější elektrické vedení v rozvodné části elektrické sítě buďto přes anténu nebo pozemní dráty. Distribuční linky nesou elektřinu střední nebo nízkonapěťovou. [31]

Cílem Evropské unie je instalace u 80 % odběratelů inteligentních měřidel do roku 2020. Přesný počet inteligentních měřidel plynu nebo energie v České Republice není dohledatelný, ale počet pro Spojené království udává počet Smart měřičů jak elektrické energie, tak plynu. Uvádí zde čtvrtletní přírůstek daných měřičů od druhé poloviny roku 2012 a celkový počet do poloviny roku 2012. Počet obou typů inteligentních měřičů, jak elektrické energie, tak plynu byl dle daných údajů do poloviny roku 2012 78 tisíc. V roce 2016 se počet měřičů vyšplhal až na hodnotu 4 979 500 inteligentních měřičů. To je zhruba 16 % všech domácností a firem, které ve Velké Británii používají již inteligentní měřiče. [32]

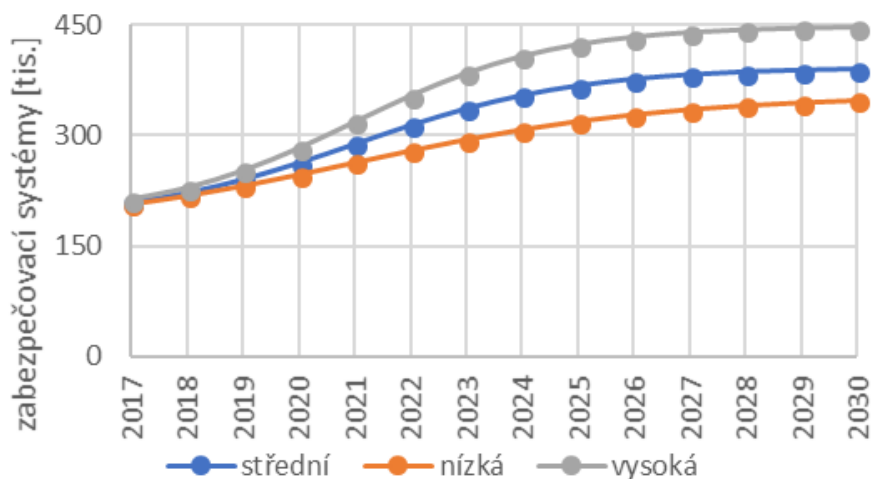


Graf 4 - Predikce počtu M2M SIM pro inteligentní měřiče

Pokud stejné procento aplikujeme i pro Českou republiku v roce 2016 by bylo 927 059 měřičů. Sice cílem Evropské unie je mít v roce 2020 nainstalováno v 80 % všech domácnostech a firem inteligentní měřiče, ale již teď se ví, že tato předpověď je nereálná. V této situaci uvažují, že 80 % všech domácností a firem dosáhne v roce 2023 při nejrychlejším růstu, a to by počet měřičů byl téměř 5 milionů. Při průměrném růstu uvažují zastoupení 80 % až v roce 2030. Ostatní predikované hodnoty pro další roky najdete v příloze, tabulka 2 – Predikce počtu M2M SIM karet pro Smart Metering. V tomto roce jsou inteligentní elektroměry instalovány pouze v některých městech České republiky a těmi jsou Pardubice, Hradec Králové, Vrchlabí a Jeřmanice. Hewlett-Packard je dodavatelem prvních 40 tisíc inteligentních měřičů pro České Energetické Závody.[33]

6.1.2.3 ZABEZPEČENÍ OBJEKTŮ

Zabezpečení domů nebo bytů jak pro soukromé osoby, tak pro firmy, prostě všech objektů je dalším využitím aplikace Machine-to-Machine. Alarmy pro zabezpečení objektů se dělí na lokální neboli místní alarmy a na monitorované. Lokální alarm je typ alarmu, který pouze vyděsí vetřelce a upozorní okolí hlasitým zvukem. Monitorované na rozdíl od těch lokální vyšlou aktivační signál do monitorovacího centra (ARC – Alarm Receiving Centre), kde jsou signály filtrovány na falešné a skutečné. Po potvrzení skutečného signálu monitorující centrum kontaktuje vlastníka objektu, či alarmu a potřebnou záchrannou službu. Monitorované alarmové systémy jsou závislé na spolehlivých komunikačních sítích. Nejnovější generace monitorovaných alarmových systémů jsou navrženy tak, aby docházelo k menšímu riziku výpadku komunikace, a tak využívají jak kabelové, tak i bezdrátové síťové připojení. Dnes je pouze 25 % všech alarmů monitorovaných ARC. Počet monitorovaných poplachových systémů v Evropě byl v roce 2016 8,7 milionů, což je pouze 3,7 % zabezpečených firem a domácností monitorovacím alarmem. Pro rok 2021 je předpoklad pro Evropu 10,6 milionů monitorovacích poplachových systémů. [34]



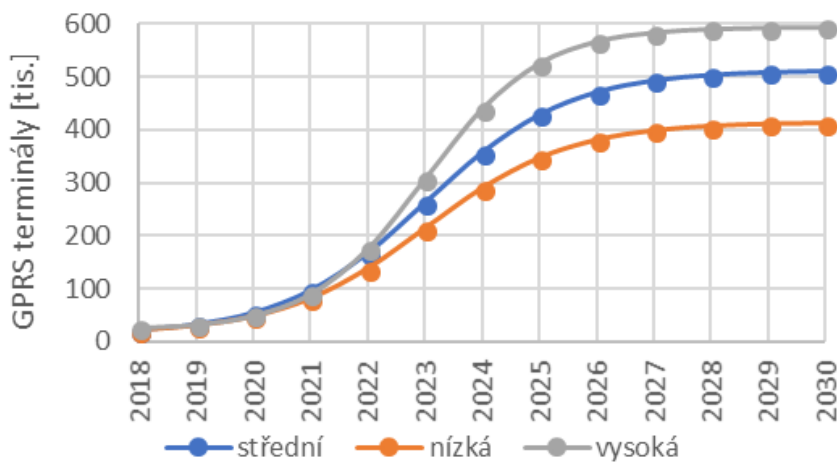
Graf 5 - Predikce počtu M2M SIM pro zabezpečovací systémy

Pro Českou republiku odpovídá 3,7 % všech domácností a firem přibližně 190 tisíc objektů, které využívají monitorovací poplachový systém. V roce 2030 by se počet zabezpečených objektů monitorovacím alarmem mohl vyšplhat až na 7 % všech objektů v České republice, což by odpovídalo počtu téměř 450 tisíc. Doplňující čísla ohledně predikce jsou viděny v příloze, tabulka 3 – Predikce počtu M2M SIM karet pro Zabezpečení objektů.

6.1.2.4 BANKOVNICTVÍ

Svět se neustále přesouvá z hotovostních plateb do elektronických forem, při kterých se čím dál více využívá bezdrátová komunikace a tím pádem i Machine-to-Machine komunikace. Součástí vývoje v bankovním sektoru jsou zejména POS terminály. POS je zkratka pro Point of Sale nebo Point of Service, jedná se o obchodní místo přijímající kartu k placení za zboží nebo služby. Velmi populární volbou pro POS terminály se stala mobilní konektivita. Bezdrátová technologie má důležitou roli při usnadňování adaptace elektronických plateb.[35]

Na trhu je již několik druhů terminálů, mezi které patří stacionární, Bluetooth, GPRS, mPOS a chytrý terminál. Nejrozšířenějším terminálem je stále stacionární terminál, který se používá v běžných prodejnách nebo provozovnách služeb. Stacionární terminál je pevně umístěný a je napájen ze sítě. Bluetooth terminál se používá v restauracích a dalších pohostinských podnicích, kde přenosný terminál urychlí a ulehčí práci zaměstnancům. Terminál komunikuje s bankou či autorizační centrálou pomocí internetu nebo GPRS modemu. GPRS terminál je typ terminálu využívající GPRS SIM karty s datovým tarifem a tím umožňuje provádět transakce pomocí datové sítě mobilního operátora kdekoli v dosahu GPRS sítě. MPOS je mobilní terminál, který komunikuje s chytrým mobilním telefonem prostřednictvím Bluetooth technologie. Nejnovějším terminálem je chytrý terminál, který obsahuje aplikace, která funguje jako pokladna a ke správě položek využívá cloudové prostředí. [36]



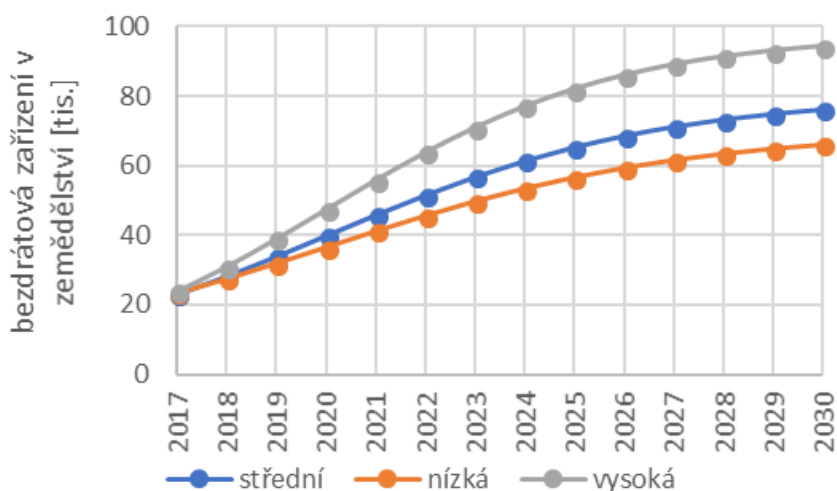
Graf 6 - Predikce počtu M2M SIM pro GPRS terminály

V roce 2015 byl počet všech bezdrátových POS terminálů 57 tisíc. [37] Všechny bezdrátové terminály ale nefungují na bázi M2M, takže pouze procento z nich jsou GPRS terminály. Počet GPRS systémů by se měl v roce 2030 pohybovat okolo 500 tisíců kusů terminálů. Pro další hodnoty týkající se predikce počtu GPRS terminálů nahlédněte do přílohy, tabulka 4 – Predikce počtu M2M SIM karet pro Bankovníctví.

6.1.2.5 ZEMĚDĚLSTVÍ

Dalším použitím Machine-to-Machine je komunikace v zemědělství. Elektronizace zemědělské techniky je každým rokem dokonalejší, avšak v posledních letech došlo ke zrychlení díky zlepšení výpočetní síly, ukládání dat a bezdrátovému přenosu dat. Inteligentní řešení v zemědělském průmyslu zahrnuje systémy instalované v zemědělských zařízeních, na poli nebo i na zvířatech. Zemědělská produkce může být pomocí těchto systémů plánovaná a řízená tak, aby dosáhla větší efektivity. Řešení v zemědělském průmyslu je automatické řízení, monitorování a kontrola zařízení prostřednictvím palubních displejů. Řešení vzdáleného monitorování zahrnují bezdrátovou konektivitu, protokolování dat, kamery a snímače, které zaznamenávají měření parametrů prostředí a podporují rozhodování v zemědělské výrobě. Příklady využití jsou například monitorování obsahu vlhkosti, existence rizika onemocnění a škůdců nebo dálkové zavlažování. V roce 2016 bylo po celém světě instalováno 17 milionu bezdrátových zařízení pro aplikaci v zemědělské výrobě a očekává se nárůst na 27,4 milionu připojených zařízení v zemědělství v roce 2021.[38]

V Evropě bylo v roce 2015 nainstalováno 7,8 milionů bezdrátových zařízení využívaných v zemědělství. Předpoklad pro rok 2020 je 14 milionů zařízení a pro rok 2025 16 milionů zařízení. [39]



Graf 7 - Predikce počtu M2M SIM pro bezdrátová zařízení v zemědělství

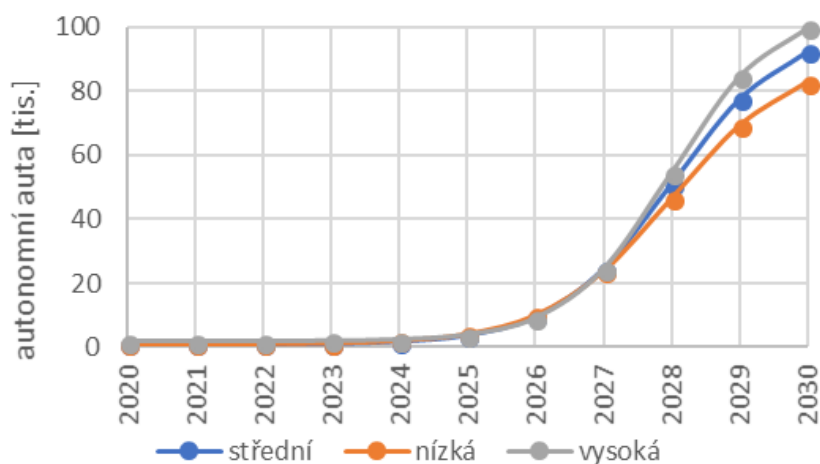
V České Republice se očekává, že počet bezdrátových zařízení využívající v zemědělském průmyslu v roce 2030 dosáhne téměř 100 tisíců kusů. Ostatní čísla týkající se počtu M2M SIM karet použitých v zemědělství je možno najít v příloze, tabulka 5 -Predikce počtu M2M SIM karet pro Zemědělství.

6.1.2.6 AUTONOMNÍ AUTA

V automobilovém průmyslu dochází k mnoha změnám, postupně vedoucím k plné automatizaci. Existuje šest úrovní automatizace aut označené od nuly do pěti, kde 0 je žádná automatizace a 5 je plná automatizace. Od úrovně 3 je auto řízeno automatickým systémem, kde je stále vyžadována reakce řidiče. K plné automatizaci dochází v úrovni 5, kde je vše řízeno automatizovaným systémem a automobil by měl obsahovat všechny způsoby řízení.[40]

Poloautonomní modely aut úrovně 2 byly uvedeny na trh v roce 2015 a dosáhly prodeje přibližně 194 tisíc vozů, předpokladem prodeje pro rok 2016 je 304 tisíc vozů a pro rok 2030 to je 43 milionů. Počet aut úrovně 3 a 4 je předpokládán, že v roce 2020 bude 200 tisíc a dosáhne 24,3 milionů v roce 2030, z čehož 16,5 milionů vozů bude úrovně 3 a zbytek úrovně 4. Předpokládá se, že auta úrovně 3 se začnou prodávat kolem roku 2020. Plně automatizovaná auta do roku 2030 pravděpodobně vůbec nebudou na trhu. [41]

Většina automobilových společností již uvedla, kdy by měli na trh přivést první autonomní auta, kde například Audi uvádí rok 2020, Ford rok 2021 a Volkswagen již rok 2019.[42]

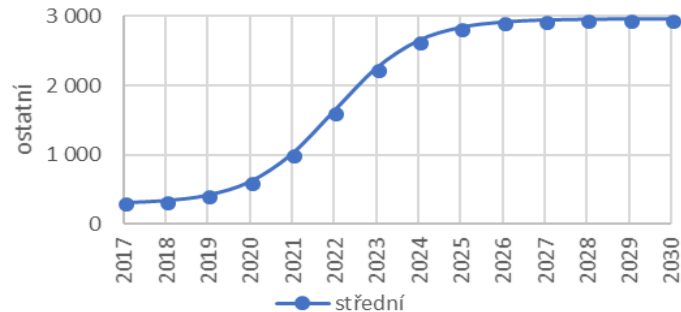


Graf 8 - Predikce počtu M2M SIM pro autonomní auta

Graf s počtem autonomních aut v České Republice nezačíná od roku 2017, jelikož nyní ještě nejsou vozidla s částečnou automatizací v prodeji. Na počátku prodeje autonomních aut úrovně 3 nebudou hodnoty počtu prodaných aut dosahovat ani jednoho tisíce. V roce 2025 začne prodej autonomních aut úrovně 4 a největší nárůst by měl začít kolem roku 2027. V roce 2030 by počet autonomních aut jak úrovně 3 tak i úrovně 4 mohl dosahovat 100 tisícům, z čehož by 70 tisíc byla auta úrovně 3 a zbylých 30 tisíc auta úrovně 4. Zbylá přibližná hodnota SIM karet využitých v autonomních autech najdeme v příloze, tabulka 6 – Predikce počtu M2M SIM karet pro Autonomní auta. Jelikož nemáme žádná předchozí data, dělá se predikce velice těžko, a proto v tomto odvětví mohou nastat největší odchylky od reality.

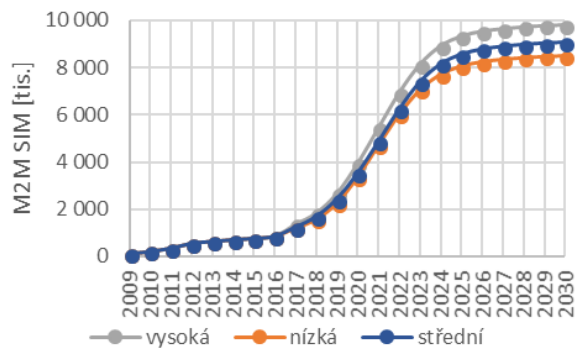
6.1.2.7 OSTATNÍ

Poslední skupina zahrnuta do konečného počtu všech M2M SIM karet, je skupina obsahující dosud nezmíněné aplikace, kde se komunikace mezi stroji používá. Tato skupina je taky velice důležitá z hlediska kompenzace nejistot týkající se trhu.



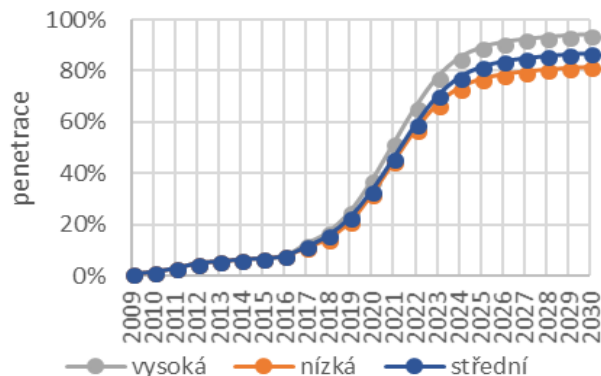
Graf 9 - Predikce počtu M2M SIM pro ostatní odvětví

Při sečtení všech podkategorií, do kterých jsem M2M SIM karty rozčlenila, dostaneme konečný počet SIM karet v oblasti Machine-to-Machine. V roce 2016 bylo pouze 838 tisíc M2M SIM karet v České Republice. Všechny hodnoty jsou uvedeny v příloze, tabulka 7 – Predikce počtu M2M SIM pro ostatní odvětví.



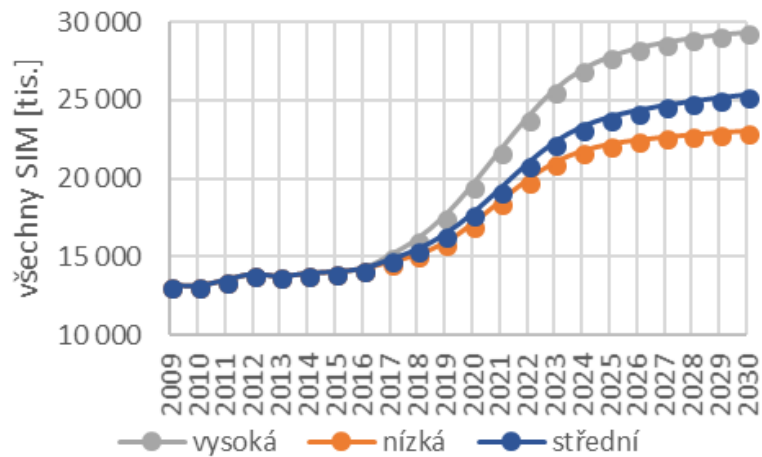
Graf 10 - Predikce počtu všech M2M SIM

Hodnota predikovaná pro rok 2030 dosahuje téměř 10 milionů. Všechna čísla jsou upřesněny v příloze, tabulka 10 - Predikce počtu M2M SIM karet. V procentuálním vyjádření, vztáhnuto na počet obyvatel dostaneme pro maximální nárůst 94 % a pro minimální nárůst 82 %.



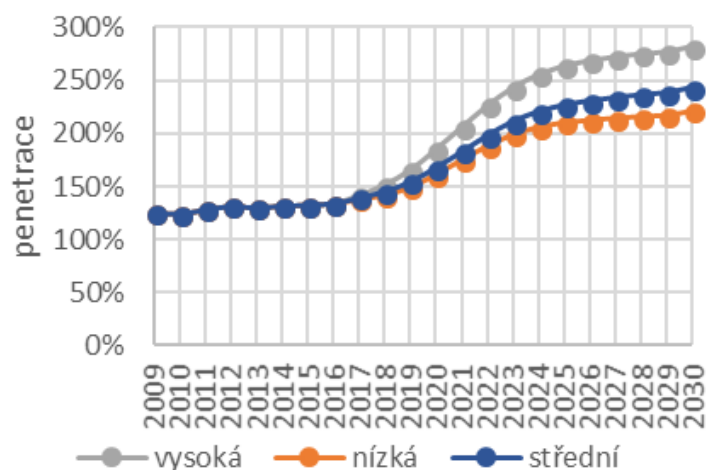
Graf 11 - Penetrace M2M SIM

Pokud spojíme počet aktivních SIM karet a M2M SIM karet dostaneme se na penetraci přesahujících 200 %. Při maximálním nárůstu je předpoklad všech karet až 30 milionů a při pomalém nárůstu odhadujeme alespoň 23 miliónu SIM karet.



Graf 12 - Predikce počtu všech SIM karet

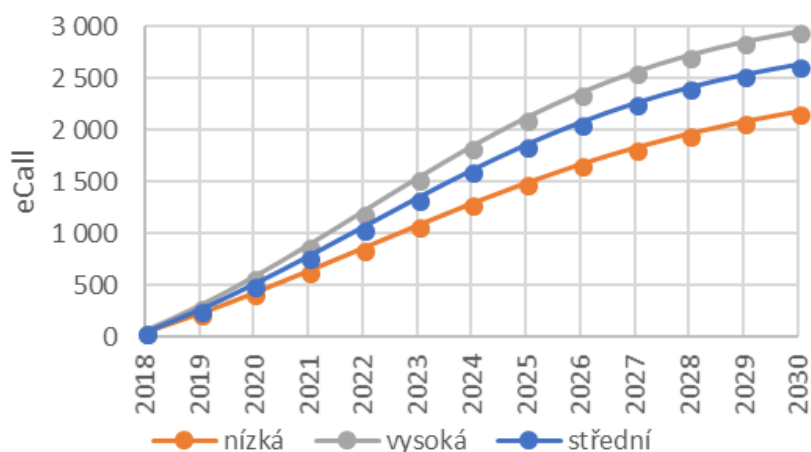
Hodnota 23 026 tisíc karet odpovídá 221 % a 29 323 tisíc je 282 %.



Graf 13 - Penetrace SIM karet (Aktivní i M2M)

6.1.3 eCALL

Jelikož není jisté, kdo ponese náklady za služby eCall, nezařadila bych tuto aplikaci přímo do SIM karet využívající Machine-to-Machine komunikaci. Systém eCall je služba, která se automaticky aktivuje, jakmile senzory ve vozidle zjistí vážnou havárii. Systém vytočí evropské číslo tísňového volání 112, vytvoří telefonní linku do příslušného střediska pro tísňová volání a pošle podrobnosti o havárii záchranným službám. Mezi položky, které by měly být zaslány záchranným službám, patří čas incidentu, přesná poloha havarujícího automobilu a směr. Ve kterém se vozidlo nachází. Pokud se systém neaktivuje automaticky může být také spuštěn ručně stisknutím tlačítka v autě, například svědkem vážné nehody. Nainstalováním systému eCall do automobilových vozidel umožníme rychlejší pomoc řidičům a cestujícím. Podle odhadu by systém mohl díky rychlejší době reakce ušetřit až 2500 životů ročně. Dne 28.4.2015 Evropský parlament odhlasoval regulaci systému eCall, kde je zavedena povinnost vybavení všech vozidel od dubna 2018 technologií eCall.[43]

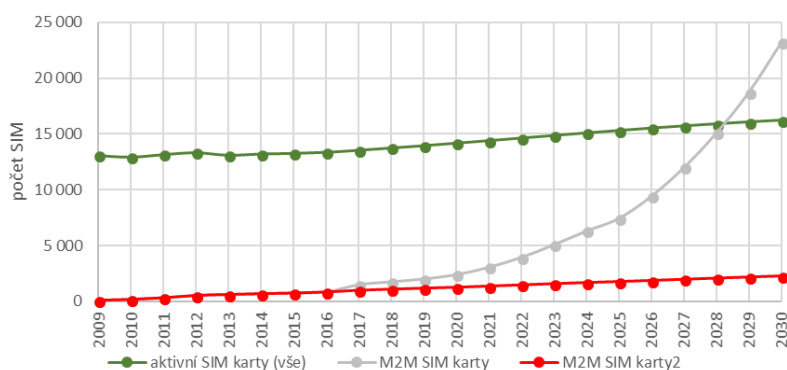


Graf 14 - Predikce systémů eCall

Hodnoty systémů eCall v automobilech začnou v roce 2018 na velmi malém počtu, jelikož jde o nově zavedený systém. Pokud procento ze všech automobilů v České Republice bude dosahovat pouze 1 % a to odpovídá hodnotě kolem 40 tisíců. V roce 2030 by mělo být zastoupení aut s eCall téměř poloviční u celkového počtu automobilů. Při maximálním nárůstu budeme uvažovat o 43 % a to jsou necelé tři milionů automobilů. Při minimálním nárůstu je odhadovaný počet 2 174 tisíc, což je přibližně 32 % ze všech automobilů v České Republice.

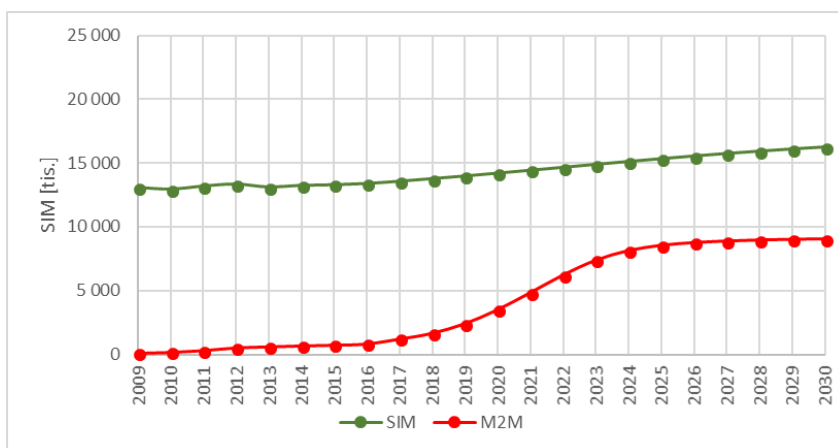
6.2 POROVNÁNÍ

Pro porovnání jsem na predikci trhu SIM karet využila funkce pomocí excelu, které jsou určeny pro predikci trhu výrobku. Do roku 2016 jsou hodnoty z Českého telekomunikačního úřadu a od roku 2017 do roku 2030 jsem zvolila funkce excelu. Na aktivní SIM karty jsem použila konkrétně funkci nabízející excelelem LINTREND. Jedná se o statistickou funkci, která se používá na predikci trhu nějakého výrobku, který je již dlouho na trhu, což SIM karty jsou. LINTREND je lineární funkce, která je založena na metodě nejmenších čtverců. Na M2M SIM karty jsem využila funkci LOGLINTREND. Funkce LOGLINTREND je také funkce, která využívá metodu nejmenších čtverců, ale jedná se o funkci logaritmickou, která je vhodnější pro predikci nového výrobku na trhu. Předpokladem je totiž, že prodej nového výrobku bude růst mnohem rychleji než výrobku, který je již na trhu dlouho. Pokud se ale podíváme na hodnoty, tak vidíme že by v následujících letech M2M SIM karty o dost převýšili normální aktivní SIM karty, což je málo pravděpodobné. Pokud tedy využijeme opět funkci LINTREND dostaneme mnohem menší hodnoty, tím pádem reálnější hodnoty.



Graf 15 - Predikce trhu

Pokud tento graf porovnáme s grafem obsahující hodnoty dle naší predikce tak vidíme, že ani jedna variant z předchozího grafu nedopovídá. Podle funkce LINTREND by v roce 2030 měl být počet M2M SIM karet 2 271 tisíc a podle LOGLINTREND 23 219 tisíc karet. Mnou predikovaná hodnota karet pro Machine-to-Machine komunikaci je při maximálním nárůstu 9 800 tisíc karet a při minimálním růstu 8 485 tisíc.



Graf 16 - Predikce trhu podle mých hodnot

7 ZÁVĚR

Cílem bakalářské práce bylo zaměřit se na relativně novou technologii, Machine-to-Machine komunikaci, která je velice spjata s internetem věcí. IoT výrazně zlepšuje interakci mezi počítačem a strojem a tím ovlivňuje zkušenosti, které jako spotřebitelé máme. Velmi důležitou částí pro Internet věcí i M2M komunikaci jsou sítě, které jsou touto technologií využívány. Každý operátor upřednostňuje jiný typ sítě, ale všichni se shodnou na nízkooenergetické rozsáhlé síti. Na výběr však v dnešní době máme již z několika sítí, mezi které patří NarrowBand IoT, speciální verze LTE mobilního internetu, SigFox, LoRa a další.

V dnešní době operátoři uvádějí několik aplikací, kde jejich nabízené M2M SIM karty s M2M tarify uplatnit. Prvním využitím Machine-to-Machine je fleet management neboli sledování služebních vozidel, kde by se hodnoty SIM karet mohly vyšplhat až na 800 tisíc. Inteligentní měřiče jsou dalším zařízením, které potřebují M2M SIM kartu a jejich četnost by mohla být téměř 90 % všech domácností a firem, což dosahuje hodnot přibližně 5 milionů. Hodnota 400 tisíc by mohl být počet monitorovaných zabezpečovacích systémů v České Republice. Pro využití v systémech používajících v zemědělském průmyslu by hodnoty měly dosahovat téměř 100 tisícům. Stejného počtu 100 tisíc by v roce 2030 měly dosahovat i autonomní auta, ale s takovým rozdílem, že u autonomních aut očekáváme rapidní nárůst až okolo roku 2025, možná později. Důležitou část M2M tvoří skupina ostatní, kde jsou zahrnuty všechny možné aplikace, které nejsou výše uvedené. Tato skupina by mohla nabývat hodnot až 3 milionu. Pokud by se zesumarizovala všechna čísla, došli bychom k celkovému počtu všech M2M karet v roce 2030 až na 10 milionů, což dává penetraci kolem 90 %. Čísla jsou již v dnešní době ohromující, i když si to možná ani neuvědomujeme, a předpokládá se, že trh tímto směrem bude jenom růst. Společnosti investují v tomto směru, jelikož doufají ve zlepšení a urychlení práce a zákazníci zkoušejí nové věci a možnosti, které Internet věcí nebo M2M komunikace nabízí. Předpověď pro technologii internetu věcí je poměrně vysoká, teď jen záleží, jestli dojde k přecenění úspěchu, jako tomu došlo v oblasti samotného internetu, kde došlo nejprve k velkému nárůstu, ale náhle potom k poklesu, díky nereálným předpokladům, neznalosti investorů či pomalému vývoji infrastruktury.

8 POUŽITÁ LITERATURA

- [1] *Y.2060 : Overview of the Internet of things* [online]. B.m.: International Telecommunication Union. červen 2012 [vid. 2017-12-10]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>
- [2] *Y.2060 : Overview of the Internet of things* [online]. [vid. 2018-05-22]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>
- [3] *Y.2067 : Common requirements and capabilities of a gateway for Internet of things applications* [online]. B.m.: International Telecommunication Union. červen 2014 [vid. 2017-12-15]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2067-201406-S>
- [4] *Y.2067 : Common requirements and capabilities of a gateway for Internet of things applications* [online]. [vid. 2018-05-21]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2067-201406-S>
- [5] *Y.2069 : Terms and definitions for the Internet of things* [online]. B.m.: International Telecommunication Union. červenec 2012 [vid. 2017-12-11]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2069-201207-I>
- [6] *Y.2077 : Requirements of the plug and play capability of the Internet of things* [online]. B.m.: International Telecommunication Union. únor 2016 [vid. 2017-12-15]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2077-201602-I>
- [7] *Y.2066 : Common requirements of the Internet of things* [online]. B.m.: International Telecommunication Union. červen 2014 [vid. 2017-12-15]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2066-201406-I>
- [8] *Y.2066 : Common requirements of the Internet of things* [online]. [vid. 2018-05-22]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2066-201406-I>
- [9] ROUTLEDGE, Lisa. *The Major difference between IoT and M2M. – IoT Roadmap* [online]. [vid. 2018-05-21]. Dostupné z: <https://www.iotroadmap.com/the-major-difference-between-iot-and-m2m/>
- [10] *ISOC-IoT-Overview-20151221-en.pdf* [online]. [vid. 2018-05-19]. Dostupné z: <https://cdn.prod.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf>
- [11] ROUTLEDGE, Lisa. *The Major difference between IoT and M2M. – IoT Roadmap* [online]. [vid. 2018-05-22]. Dostupné z: <https://www.iotroadmap.com/the-major-difference-between-iot-and-m2m/>
- [12] *F.748.5 : Requirements and reference architecture of the machine-to-machine service layer* [online]. B.m.: International Telecommunication Union. listopad 2015 [vid. 2017-12-16]. Dostupné z: <https://www.itu.int/rec/T-REC-F.748.5-201511-I>
- [13] *F.748.5 : Requirements and reference architecture of the machine-to-machine service layer* [online]. [vid. 2018-05-22]. Dostupné z: <https://www.itu.int/rec/T-REC-F.748.5-201511-I>
- [14] *Q.3052 : Overview of application programming interfaces and protocols for the machine-to-machine service layer* [online]. B.m.: International Telecommunication Union. únor 2016 [vid. 2017-12-17]. Dostupné z: <https://www.itu.int/rec/T-REC-Q.3052-201602-I>
- [15] *Y.4455 : Reference architecture for Internet of things network service capability exposure* [online]. B.m.: International Telecommunication Union. říjen 2017 [vid. 2017-12-18]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.4455-201710-I>

- [16] *Y.4455 : Reference architecture for Internet of things network service capability exposure* [online]. [vid. 2018-05-22]. Dostupné z: <https://www.itu.int/rec/T-REC-Y.4455-201710-I>
- [17] TECHNIKY, České vysoké učení technické v Praze Katedra telekomunikační. *Access Server* [online]. [vid. 2018-05-19]. Dostupné z: <http://access.feld.cvut.cz/view.php?cisloclanku=2004072801>
- [18] 3GPP - Description Releases. *3GPP* [online]. [vid. 2018-01-25]. Dostupné z: http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/
- [19] AB, Ericsson. Cellular networks for Massive IoT – enabling low power wide area applications. nedatováno, 13.
- [20] Low-Power Wide-Area (LPWA) technology. *M2M Alliance* [online]. 17. listopad 2016 [vid. 2018-05-21]. Dostupné z: <http://www.m2m-alliance.com/en/low-power-wide-area-lpwa-technology/>
- [21] LIBERG, Olof. Cellular Internet of Things. *3GPP* [online]. říjen 2017 [vid. 2018-03-05]. Dostupné z: <http://www.3gpp.org/ciot>
- [22] Narrowband IoT (NB-IoT) | u-blox. *U-blox* [online]. únor 2018 [vid. 2018-03-05]. Dostupné z: <https://www.u-blox.com/en/narrowband-iot-nb-iot-0>
- [23] SARA-N2 series | u-blox. *U-blox* [online]. [vid. 2018-03-05]. Dostupné z: <https://www.u-blox.com/en/product/sara-n2-series>
- [24] EVK-N2. *u-blox* [online]. 9. srpen 2017 [vid. 2018-05-17]. Dostupné z: <https://www.u-blox.com/en/product/evk-n2>
- [25] *Sigfox-technical-overview-July-2017.pdf* [online]. [vid. 2018-05-17]. Dostupné z: <https://simplecell.eu/wp-content/uploads/2018/01/Sigfox-technical-overview-July-2017.pdf>
- [26] *simplecell.eu – Connecting Things* [online]. [vid. 2018-04-04]. Dostupné z: <https://simplecell.eu/>
- [27] *Talk-Rescom-16-LPWAN-review.pdf* [online]. [vid. 2018-05-17]. Dostupné z: <http://cpham.perso.univ-pau.fr/Paper/Talk-Rescom-16-LPWAN-review.pdf>
- [28] *cvut-ctuocneni9001800mhz-final.pdf* [online]. [vid. 2018-05-20]. Dostupné z: <https://www.ctu.cz/sites/default/files/obsah/ctu/vyzva-k-uplatneni-pripominek-k-zameru-ctu-udelit-pridel-radiovych-kmitoctu-v-kmitoctovych-pasmech.1-zakona-o-elektronickych-komunikacich/obrazky/cvut-ctuocneni9001800mhz-final.pdf>
- [29] *bi-fm8-ps.pdf* [online]. [vid. 2018-05-17]. Dostupné z: <http://www.berginsight.com/reportpdf/productsheet/bi-fm8-ps.pdf>
- [30] *bi-fm12-ps.pdf* [online]. [vid. 2018-05-17]. Dostupné z: <http://berginsight.com/ReportPDF/ProductSheet/bi-fm12-ps.pdf>
- [31] *T-TUT-HOME-2010-PDF-E.pdf* [online]. [vid. 2018-05-17]. Dostupné z: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-HOME-2010-PDF-E.pdf
- [32] Statistical release and data: Smart Meters, Great Britain, quarter 4 2017. *GOV.UK* [online]. [vid. 2018-04-20]. Dostupné z: <https://www.gov.uk/government/statistics/statistical-release-and-data-smart-meters-great-britain-quarter-4-2017>
- [33] WEBDESIGN, FG Forrest, a s , fg {zavináč} fg {tečka} cz-Content Management System- Edee CMS; SYMBIO Digital, s r o-. Info k pilotnímu projektu inteligentního měření | Výzkum a vývoj | Skupina ČEZ. *ČEZ* [online]. [vid. 2018-04-25]. Dostupné z: <https://www.cez.cz/cs/vyzkum-a->

vzdelavani/vyzkum-a-vyvoj/subjekty-v-oblasti-vyzkumu-a-vyvoje/eu-verejne-zdroje-financovani/smart-grids/info-k-pilotnimu-projektu-inteligentniho-mereni.html

- [34] *bi-security8-ps.pdf* [online]. [vid. 2018-05-17]. Dostupné z: <http://www.berginsight.com/ReportPDF/ProductSheet/bi-security8-ps.pdf>
- [35] *bi-pos2-ps.pdf* [online]. [vid. 2018-05-17]. Dostupné z: <http://www.berginsight.com/ReportPDF/ProductSheet/bi-pos2-ps.pdf>
- [36] Platební terminály. *Platební terminály* [online]. [vid. 2018-05-01]. Dostupné z: <http://www.platebniterminaly.eu/>
- [37] S.R.O, IPC Corporation. Platební terminály zvyšují restauracím tržby až o 30%. *Investujeme.cz* [online]. březen 2015 [vid. 2018-05-01]. Dostupné z: <https://www.investujeme.cz/tiskove-zpravy/platebni-terminaly-zvysuji-restauracim-trzby-az-o-30/>
- [38] *bi-agriculture-ps.pdf* [online]. [vid. 2018-05-17]. Dostupné z: <http://www.berginsight.com/ReportPDF/ProductSheet/bi-agriculture-ps.pdf>
- [39] TAX, * All products require an annual contract Prices do not include sales. Agriculture IoT EU 2017-2025 | Statistic. *Statista* [online]. [vid. 2018-05-02]. Dostupné z: <https://www.statista.com/statistics/691880/agriculture-iot-units-in-the-eu/>
- [40] Figure 1 : SAE International: six levels of driving automation (SAE... *ResearchGate* [online]. [vid. 2018-05-17]. Dostupné z: https://www.researchgate.net/figure/SAE-International-six-levels-of-driving-automation-SAE-International-2014-Center-for_fig1_287829194
- [41] *bi-autonomous-ps.pdf* [online]. [vid. 2018-05-17]. Dostupné z: <http://www.berginsight.com/ReportPDF/ProductSheet/bi-autonomous-ps.pdf>
- [42] *Forecasts | Driverless car market watch* [online]. [vid. 2018-05-17]. Dostupné z: http://www.driverless-future.com/?page_id=384
- [43] European Commission - PRESS RELEASES - Press release - eCall: automated emergency call for road accidents mandatory in cars from 2015. *Europa* [online]. červen 2013 [vid. 2018-05-02]. Dostupné z: http://europa.eu/rapid/press-release_IP-13-534_en.htm

PŘÍLOHY

Tabulka 1 - Predikce počtu M2M SIM karet pro Fleet Managment

Sledování pohybu aut(tis.)		2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
vysoká	penetrace										3%	3%	4%	5%	6%	7%	8%	9%	9%	10%	10%	10%	9%
	přírusek										82%	23%	26%	26%	23%	19%	14%	10%	7%	4%	3%	2%	1%
	počet										179	222	279	352	433	515	587	645	687	716	735	747	755
střední	penetrace	0%	0%	1%	1%	1%	1%	1%	1%	2%	2%	3%	3%	4%	5%	5%	6%	6%	7%	7%	7%	7%	7%
	přírusek		66%	40%	29%	16%	15%	11%	9%	32%	37%	25%	25%	24%	21%	17%	14%	10%	7%	5%	3%	2%	2%
	počet	15	25	36	46	54	62	69	75	99	135	169	211	261	316	370	420	463	496	522	540	553	561
nízká	penetrace										2%	2%	3%	3%	4%	4%	5%	5%	5%	5%	5%	6%	6%
	přírusek										26%	21%	21%	20%	18%	15%	12%	9%	7%	5%	4%	3%	2%
	počet										124	150	181	217	255	293	329	360	386	406	421	432	441

Tabulka 2 - Predikce počtu M2M SIM karet pro Smart Metering

Smart Metering(tis.)		2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
vysoká	penetrace									12%	18%	30%	47%	63%	74%	80%	82%	83%	83%	83%	83%	82%	82%
	přírusek									258%	53%	65%	56%	36%	18%	8%	4%	1%	1%	0%	0%	0%	0%
	počet									688	1 055	1 740	2 721	3 702	4 387	4 754	4 923	4 995	5 026	5 038	5 043	5 045	5 046
střední	penetrace	0%	0%	0%	0%	1%	1%	2%	3%	10%	16%	26%	40%	54%	64%	69%	72%	73%	74%	73%	73%	73%	73%
	přírusek		42%	43%	173%	132%	137%	41%	68%	195%	64%	65%	53%	35%	19%	10%	5%	2%	1%	0%	0%	0%	0%
	počet	3	4	5	15	34	81	114	192	567	928	1 532	2 340	3 149	3 753	4 114	4 301	4 392	4 433	4 452	4 461	4 465	4 467
nízká	penetrace									9%	14%	23%	38%	52%	61%	65%	67%	67%	67%	67%	67%	66%	66%
	přírusek									180%	50%	68%	62%	38%	18%	8%	3%	1%	0%	0%	0%	0%	0%
	počet									538	809	1 363	2 204	3 045	3 598	3 870	3 983	4 028	4 045	4 052	4 054	4 055	4 055

Tabulka 3 - Predikce počtu M2M SIM karet pro Zabezpečení objektů

Zabezpečení objektů(tis.)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
vysoká	penetrace								4%	4%	5%	5%	6%	6%	7%	7%	7%	7%	7%	7%	7%	7%
	přírůstek								25%	7%	10%	12%	13%	11%	9%	6%	4%	2%	1%	1%	0%	0%
	počet								213	229	252	283	318	354	384	407	423	433	439	443	445	446
střední	penetrace	2%	2%	2%	3%	3%	3%	3%	4%	4%	4%	5%	5%	5%	6%	6%	6%	6%	6%	6%	6%	6%
	přírůstek		40%	14%	15%	9%	5%	6%	1%	23%	6%	8%	9%	10%	9%	7%	5%	4%	2%	2%	1%	1%
	počet	76	106	121	139	152	160	169	171	210	223	241	263	289	314	336	354	367	376	382	386	388
nízká	penetrace								4%	4%	4%	4%	5%	5%	5%	5%	5%	6%	6%	6%	6%	6%
	přírůstek								21%	5%	6%	7%	7%	6%	5%	5%	4%	3%	2%	2%	1%	1%
	počet								208	219	232	247	264	280	295	308	320	329	336	341	345	348

Tabulka 4 - Predikce počtu M2M SIM karet pro Bankovníctví

Bankovníctví (tis.)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
vysoká	penetrace									10%	10%	13%	20%	32%	47%	56%	56%	56%	53%	50%	46%	43%
	přírůstek									82%	24%	51%	82%	94%	75%	43%	19%	8%	3%	1%	0%	0%
	počet									27	33	50	91	177	309	441	526	567	584	590	593	594
střední	penetrace	4%	4%	4%	4%	6%	6%	6%	7%	8%	10%	14%	21%	31%	40%	45%	45%	46%	45%	42%	40%	37%
	přírůstek		11%	5%	12%	9%	92%	30%	7%	51%	47%	49%	69%	78%	74%	57%	36%	20%	10%	5%	2%	1%
	počet	3	3	3	3	4	7	9	10	15	21	32	54	96	168	263	357	429	471	493	504	508
nízká	penetrace									8%	9%	12%	18%	25%	33%	37%	37%	37%	36%	34%	32%	30%
	přírůstek									45%	40%	59%	72%	70%	55%	36%	20%	10%	5%	2%	1%	0%
	počet									21	30	47	81	138	214	290	347	381	398	407	411	413

Tabulka 5 - Predikce počtu M2M SIM karet pro Zemědělství

Zemědělství (tis.)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
vysoká	penetrace									0,15%	0,17%	0,19%	0,20%	0,22%	0,24%	0,25%	0,26%	0,26%	0,26%	0,26%	0,26%	0,25%
	přírůstek									34,6%	25,6%	21,5%	17,7%	14,2%	11,2%	8,6%	6,5%	4,8%	3,5%	2,6%	1,9%	1,3%
	počet									24	31	39	48	56	64	71	77	82	86	89	91	93
střední	penetrace	0,12%	0,08%	0,08%	0,08%	0,08%	0,09%	0,10%	0,11%	0,12%	0,13%	0,15%	0,16%	0,17%	0,18%	0,19%	0,20%	0,21%	0,21%	0,21%	0,21%	0,20%
	přírůstek		33,3%	32,8%	32,1%	31,2%	30,0%	28,6%	26,9%	24,9%	22,6%	20,1%	17,5%	14,9%	12,4%	10,1%	8,1%	6,4%	5,0%	3,8%	2,9%	2,2%
	počet	3	4	5	7	9	11	15	19	23	28	34	40	46	52	57	61	65	69	71	73	75
nízká	penetrace									0,13%	0,14%	0,14%	0,15%	0,16%	0,17%	0,17%	0,18%	0,18%	0,18%	0,18%	0,18%	0,18%
	přírůstek									26,6%	17,6%	16,2%	14,5%	12,6%	10,8%	9,0%	7,4%	6,0%	4,8%	3,8%	2,9%	2,3%
	počet									23	28	32	37	41	46	50	54	57	60	62	64	65

Tabulka 6 - Predikce počtu M2M SIM karet pro Autonomní auta

Autonomní auta (tis.)		2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
vysoká	penetrace												0,03%	0,03%	0,03%	0,03%	0,03%	0,05%	0,12%	0,32%	0,71%	1,08%	1,25%
	přírusek													0,5%	1,7%	6,1%	21,0%	62,4%	132,0%	167,4%	123,4%	55,2%	18,1%
	počet												2	2	2	2	2	4	9	24	54	85	100
střední	penetrace												0,02%	0,02%	0,02%	0,02%	0,03%	0,05%	0,13%	0,33%	0,66%	0,99%	1,16%
	přírusek													1,8%	5,7%	17,4%	47,9%	102,8%	152,1%	154,5%	108,1%	52,0%	19,2%
	počet												1	1	1	1	2	4	10	25	51	77	92
nízká	penetrace												0,02%	0,02%	0,02%	0,02%	0,03%	0,06%	0,14%	0,31%	0,61%	0,89%	1,04%
	přírusek													2,7%	7,9%	21,9%	53,5%	101,4%	137,8%	135,4%	96,0%	49,0%	19,7%
	počet												1	1	1	1	2	4	10	24	46	69	83

Tabulka 7 - Predikce počtu M2M SIM pro ostatní odvětví

Ostatní		2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
střední	penetrace	0,07%	0,35%	1,45%	3,07%	3,44%	3,48%	3,49%	3,52%	3,72%	4,00%	4,74%	6,52%	10,22%	15,95%	21,69%	25,43%	27,24%	28,01%	28,33%	28,47%	28,55%	28,60%
	přírusek		424,98%	318,62%	111,75%	11,96%	1,37%	0,39%	0,96%	6,01%	7,44%	18,06%	37,30%	56,68%	55,82%	35,82%	17,09%	7,00%	2,68%	1,00%	0,37%	0,14%	0,05%
	počet	7	36	153	323	362	367	368	372	394	423	500	686	1 075	1 675	2 275	2 664	2 851	2 927	2 957	2 968	2 972	2 973

Tabulka 8 - Predikce počtu systémů eCall

eCall		2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
vysoká	penetrace										1%	5%	10%	15%	20%	25%	30%	34%	37%	39%	41%	42%	43%
	přírusek											473%	95%	54%	37%	27%	20%	15%	11%	9%	6%	5%	4%
	počet										51	293	572	880	1 204	1 528	1 836	2 115	2 357	2 559	2 723	2 852	2 952
střední	penetrace										1%	5%	9%	13%	18%	22%	26%	30%	33%	35%	36%	38%	38%
	přírusek											502%	95%	53%	36%	27%	20%	15%	12%	9%	7%	5%	4%
	počet										43	261	507	776	1 057	1 338	1 606	1 853	2 070	2 255	2 408	2 532	2 630
nízká	penetrace										1%	4%	8%	11%	15%	18%	21%	24%	26%	28%	30%	31%	32%
	přírusek											390%	88%	50%	34%	26%	20%	15%	12%	10%	8%	6%	5%
	počet										46	227	425	637	856	1 075	1 287	1 485	1 666	1 825	1 962	2 078	2 174

Tabulka 9 - Predikce počtu všech SIM karet mimo M2M SIM karty

SIM karty (mimo M2M)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	
vysoká	penetrace	124%	123%	125%	127%	125%	126%	126%	126%	130%	135%	142%	148%	155%	161%	167%	172%	176%	180%	182%	185%	186%	188%
	přírůstek		-1,07%	1,81%	1,23%	-1,68%	0,92%	0,35%	0,74%	2,62%	4,16%	4,48%	4,51%	4,32%	3,94%	3,43%	2,88%	2,34%	1,85%	1,43%	1,09%	0,82%	0,61%
	počet	13 075	12 934	13 168	13 330	13 105	13 226	13 273	13 370	13 721	14 292	14 932	15 607	16 281	16 921	17 502	18 006	18 428	18 769	19 037	19 245	19 403	19 522
střední	penetrace	124%	123%	125%	127%	125%	126%	126%	126%	128%	130%	132%	135%	137%	139%	142%	144%	146%	149%	151%	153%	154%	156%
	přírůstek		-1,07%	1,81%	1,23%	-1,68%	0,92%	0,35%	0,74%	1,38%	1,46%	1,53%	1,58%	1,60%	1,60%	1,57%	1,52%	1,46%	1,37%	1,28%	1,17%	1,07%	0,96%
	počet	13 075	12 934	13 168	13 330	13 105	13 226	13 273	13 370	13 555	13 753	13 963	14 183	14 410	14 640	14 870	15 097	15 317	15 527	15 725	15 910	16 080	16 234
nízká	penetrace	124%	123%	125%	127%	125%	126%	126%	126%	127%	128%	129%	130%	131%	132%	133%	134%	135%	136%	137%	138%	139%	140%
	přírůstek		-1,07%	1,81%	1,23%	-1,68%	0,92%	0,35%	0,74%	0,73%	0,55%	0,56%	0,58%	0,59%	0,60%	0,61%	0,61%	0,61%	0,61%	0,61%	0,60%	0,59%	0,58%
	počet	13 075	12 934	13 168	13 330	13 105	13 226	13 273	13 370	13 467	13 541	13 617	13 695	13 776	13 859	13 943	14 028	14 114	14 200	14 286	14 372	14 457	14 541

Tabulka 10 – Predikce počtu všech M2M SIM karet

M2M SIM karty	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	
vysoká	penetrace	1%	2%	3%	5%	6%	7%	7%	8%	13%	17%	25%	37%	52%	66%	78%	85%	89%	91%	92%	93%	94%	94%
	přírůstek		67,70%	80,76%	65,16%	15,14%	12,10%	8,11%	12,61%	59,38%	36,19%	45,87%	47,97%	38,60%	27,28%	17,43%	9,59%	4,65%	2,17%	1,14%	0,80%	0,57%	0,30%
	počet	106	179	323	533	614	688	744	838	1 335	1 819	2 653	3 926	5 441	6 925	8 132	8 913	9 327	9 529	9 638	9 715	9 771	9 801
střední	penetrace	1%	2%	3%	5%	6%	7%	7%	8%	12%	16%	23%	33%	46%	59%	70%	78%	82%	84%	85%	86%	87%	87%
	přírůstek		67,70%	80,76%	65,16%	15,14%	12,10%	8,11%	12,61%	46,14%	36,97%	44,76%	45,04%	37,81%	28,38%	18,53%	10,22%	5,08%	2,51%	1,37%	0,91%	0,63%	0,35%
	počet	106	179	323	533	614	688	744	838	1 224	1 677	2 428	3 521	4 853	6 230	7 384	8 139	8 553	8 767	8 887	8 968	9 024	9 056
nízká	penetrace	1%	2%	3%	5%	6%	7%	7%	8%	11%	15%	21%	32%	45%	57%	67%	73%	77%	79%	80%	81%	81%	82%
	přírůstek		67,70%	80,76%	65,16%	15,14%	12,10%	8,11%	12,61%	40,68%	31,79%	44,54%	49,59%	40,05%	27,67%	17,28%	9,33%	4,57%	2,24%	1,24%	0,84%	0,59%	0,36%
	počet	106	179	323	533	614	688	744	838	1 179	1 553	2 245	3 359	4 704	6 005	7 043	7 700	8 052	8 233	8 335	8 405	8 455	8 485

Tabulka 11 - Predikce počtu všech SIM karet

Všechny aktivní SIM	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	
vysoká	penetrace	126%	125%	129%	132%	131%	132%	133%	134%	142%	152%	166%	185%	206%	226%	243%	256%	264%	269%	272%	275%	277%	282%
	přírůstek		-1%	3%	3%	-1%	1%	1%	1%	6%	7%	9%	11%	11%	10%	7%	5%	3%	2%	1%	1%	1%	1%
	počet	13 181	13 113	13 490	13 863	13 719	13 914	14 017	14 208	15 056	16 110	17 585	19 532	21 721	23 847	25 635	26 919	27 754	28 298	28 676	28 961	29 174	29 323
střední	penetrace	126%	125%	129%	132%	131%	132%	133%	134%	140%	146%	155%	168%	183%	198%	211%	221%	227%	231%	234%	236%	238%	243%
	přírůstek		-1%	3%	3%	-1%	1%	1%	1%	4%	4%	6%	8%	9%	8%	7%	4%	3%	2%	1%	1%	1%	1%
	počet	13 181	13 113	13 490	13 863	13 719	13 914	14 017	14 208	14 779	15 430	16 391	17 705	19 263	20 870	22 254	23 236	23 869	24 294	24 612	24 878	25 104	25 290
nízká	penetrace	126%	125%	129%	132%	131%	132%	133%	134%	138%	143%	150%	162%	175%	189%	199%	206%	210%	213%	215%	216%	218%	221%
	přírůstek		-1%	3%	3%	-1%	1%	1%	1%	3%	3%	5%	8%	8%	7%	6%	4%	2%	1%	1%	1%	1%	0%
	počet	13 181	13 113	13 490	13 863	13 719	13 914	14 017	14 208	14 646	15 094	15 862	17 054	18 480	19 864	20 986	21 728	22 166	22 433	22 621	22 777	22 912	23 026