VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

# BAKALÁŘSKÁ PRÁCE

Brno, 2016 Tomáš Uher


# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

## ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS


# KOMERČNÍ MOBILNÍ SÍTĚ JAKO KRITICKÁ INFRASTRUKTURA
COMMERCIAL CELLULAR NETWORKS FOR CRITICAL INFRASTRUCTURE

**BAKALÁŘSKÁ PRÁCE**
BACHELOR'S THESIS


**AUTOR PRÁCE** — **Tomáš Uher**
AUTHOR

**VEDOUCÍ PRÁCE** — **Ing. Radko Krkoš**
SUPERVISOR



**BRNO 2016**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

# Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

***Student:*** Tomáš Uher ***ID:*** 133893
***Ročník:*** 3 ***Akademický rok:*** 2015/16

**NÁZEV TÉMATU:**

## Komerční mobilní sítě jako kritická infrastruktura

**POKYNY PRO VYPRACOVÁNÍ:**

Popište po technické stránce možnosti využití komerčních mobilních sítí pro podporu kritické infrastruktury pro zabezpečení základních funkcí a strategických zájmů státu, potřeby veřejného sektoru, ale také podporu kritické infrastruktury výroby, průmyslu a služeb. Analyzujte speciální požadavky na systémy podporující kritickou infrastrukturu, zabezpečení a ověřování splnění těchto požadavků. Diskutujte možnost využití komerčních mobilních sítí v případě mimořádné události a možnosti podpory speciálních požadavků pro zabezpečení funkcí kritické infrastruktury, prioritizaci a koexistenci s komerčním provozem a službami. Analyzujte možnost podpory komunikace kritických koncových zařízení v experimentální mobilní síti na UTKO FEKT VUT v Brně.

**DOPORUČENÁ LITERATURA:**

[1] Private LTE for Critical Infrastructure [online]. In: . Motorola, ENTELEC, 2013. Dostupné z: https://higherlogicdownload.s3.amazonaws.com/ENTELECCOMMUNITY/44abb782-c5b--4380-8cad-18966390f503/UploadedImages/Private LTE for Critical Infrastructure.pdf

[2] ČESKÁ REPUBLIKA. Zákon o krizovém řízení a o změně některých zákonů: Krizový zákon. In: . 2000. 240/2000 Sb. Dostupné také z: https://portal.gov.cz/app/zakony/download?idBiblio=49557

***Termín zadání:*** 1.2.2016 ***Termín odevzdání:*** 1.6.2016

***Vedoucí práce:*** Ing. Radko Krkoš
***Konzultant bakalářské práce:***

**doc. Ing. Jiří Mišurec, CSc.**, *předseda oborové rady*

**ANOTACE**

Tato bakalářská práce pojednává o možnostech využití komerčních mobilních sítí pro podporu kritické infrastruktury státu, výroby a služeb. Dále se zabývá speciálními požadavky na tyto systémy. Poslední část bakalářské práce se zabývá možnostmi podpory komunikace kritických koncových zařízení v experimentální mobilní síti UTKO.

**KLÍČOVÁ SLOVA**

Kritická infrastruktura, komerční mobilní síť, mimořádná událost, TETRA, IZS, tísňové volání, Iperf

**ABSTRACT**

This bachelor thesis discusses the possibilities of using commercial celluar networks to support the critical infrastructure of state, manufacturing and services. It also focus on special requirements for these systems. The last part of bachelor thesis deals with possibilites of support comummunication crtical end devices in the experimental celluar network of UTKO

**KEYWORDS**

Critical infrastructure, commercial celluar network, emergency, TETRA, emergency service, emergency telephone number

UHER, T. *Komerční mobilní sítě jako kritická infrastruktura.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2016. 53 s. Vedoucí bakalářské práce Ing. Radko Krkoš.

# Prohlášení

Prohlašuji, že svou bakalářskou práci na téma „Komerční mobilní sítě jako kritická infrastruktura“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ……. .....

podpis autora

# Poděkování

Děkuji vedoucímu bakalářské práce Ing. Radkovi Krkošovi, za velmi užitečnou metodickou pomoc a cenné rady a podnětné návrhy při zpracování bakalářské práce.


V Brně dne ……..  .....

podpis autora

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering and Communication
Brno University of Technology
Technicka 12, CZ-61600 Brno, Czechia
http://www.six.feec.vutbr.cz

Výzkum popsaný v této bakalářské práci byl realizovaný v laboratořích podpořených projektem Centrum senzorických, informačních a komunikačních systémů (SIX); registrační číslo CZ.1.05/2.1.00/03.0072, operačního programu Výzkum a vývoj pro inovace

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

# Obsah

# Seznam obrázků



# Seznam tabulek

# Úvod

Moderní informační a komunikační technologie se staly nedílnou součásti našich životů a obklopují nás téměř na každém kroku. Komerční mobilní sítě už dávno neslouží pouze k uskutečňování telefonních hovorů a posílání textových zpráv. S jejich neustálým vývojem se zvětšuje míra jejich využití i v aspektech, kde do dnes nehrály významnou roli. Jejich přínos nachází využití v mnohem strukturovanějších celcích jako je celková infrastruktura státu.

Kritická infrastruktura státu je komplexní systém služeb a zařízení podílející se na chodu státu. Při narušení funkce některé z těchto služeb nelze vyloučit kolaps chodu celého státu. Proto se stát jako správní orgán snaží zvýšit odolnost těchto systémů. Jednou z cest dosáhnutí cíle je implementace komunikačních a informačních systémů do systému kritické infrastruktury.

Tato bakalářská práce se zabývá možnostmi využití komerčních mobilních sítí pro podporu kritické infrastruktury státu, tedy pro zabezpečení základních funkcí a strategických zájmů. Dále jsou analyzovány speciální požadavky na systémy podporující kritickou infrastrukturu. Jsou zde diskutovány možnosti využití komerčních mobilních sítí v případě mimořádné události. V poslední části práce jsou analyzovány možnosti podpory komunikace kritických koncových zařízení v experimentální mobilní sítí UTKO FEKT VUT v Brně.

# 1 Kritická infrastruktura

Krizový zákon – Zákon 240/2000 Sb. O krizovém řízení a změně některých zákonů stanovuje působnost a pravomoc orgánů územních samosprávných celků, práva a povinnosti právnických a fyzických osob při přípravě krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením a při jejich řešení.

Ochrana kritické infrastruktury znamená snížení zranitelnosti jednotlivých prvků k dosažení vyšší stability celého systému. Principem je vypracování technologických řešení vedoucích k zmírnění a co nejrychlejší nápravě vzniklých škod. Základním předpokladem je nalezení preventivních opatření, primárně zvýšení odolnosti prvků kritické infrastruktury proti vzniku mimořádné události.

Ochrana kritické infrastruktury je jedním ze základních cílů každého státu. Ne všechny prvky kritické infrastruktury však spadají majetkově pod správu státu. Mnoho prvků kritické infrastruktury mají na starost soukromé subjekty, jako například dodavatelé energií a pohonných hmot. V České republice zodpovídá za problematiku kritické infrastruktury Výbor pro civilní a nouzové plánování, který organizačně spadá pod Bezpečnostní radu státu České republiky. Jednotlivá ministerstva mají na starost chod pod jejich správu spadajících prvků kritické infrastruktury a přijímat opatření k jejímu zachování.

Pro pochopení problematiky kritické infrastruktury je třeba vycházet z následujících definic [11]:

- **Kritická infrastruktura** – prvek nebo systém prvků, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.
- **Evropská kritická infrastruktura** – kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie.
- **Prvek kritické infrastruktury –** zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií. Je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury.
- **Ochrana kritické infrastruktury –** opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury
- **Subjekt kritické infrastruktury** – provozovatel prvku kritické infrastruktury. Jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury.
- **Průřezové kritéria -** soubor hledisek pro posuzování závažnosti vlivu narušení funkce prvku kritické infrastruktury s mezními hodnotami, které zahrnují rozsah ztrát na životě, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života.
- **Odvětvové kritéria –** technické nebo provozní hodnoty k určování prvku kritické infrastruktury v odvětvích energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa

## 1.1 Prvky kritické infrastruktury

Charakteristickým prvkem kritické infrastruktury je vzájemná propojenost dvou a více systémů, které dohromady tvoří síť. Narušení jednoho ze systémů tak může mít bezprostřední dopad na systémy s ním propojené. Výpadek více systémů může způsobit zhroucení celé kritické infrastruktury. Z tohoto důvodu je nutno na tyto systémy pohlížet nejen jako na samostatné celky. Propojenost mezi systémy kritické infrastruktury dělíme podle charakteru jejich závislosti na fyzickou, logickou, územní a kybernetickou [6]:

- Materiální závislost – Dvě infrastruktury jsou fyzicky závislé, pokud je stav první závislý na materiálním výstupu druhé.
- Geografická závislost – Infrastruktury jsou geograficky vzájemně závislé, pokud událost na území první infrastruktury má vliv na funkčnost druhé infrastruktury.
- Kybernetická závislost – Stav infrastruktury závisí na informacích přenášených informační infrastrukturou, například informační systémy a systémy řízení.
- Logická závislost – Závislost dvou infrastruktur nespadá do žádné z výše zmíněných. Jedná se především o předpisy, finance a legislativa.

Prvky kritické infrastruktury se v České republice podle rozhodnutí Bezpečnostní rady státu dělí podle výše zmíněných odvětvových kritérií do devíti oblastí a v jejich rámci do 37 produktů a služeb, které jsou shrnuty do tabulky 1.1 [11]:

Tabulka 1.1 Oblasti kritické infrastruktury

| P. č. | Oblast Kritické infrastruktury | Produkty a služby | |
|---|---|---|---|
| 1. | Energetika | 1.1. | Elektřina |
| | | 1.2. | Plyn |
| | | 1.3. | Tepelná energie |
| | | 1.4. | Ropa a ropné produkty |
| 2. | Vodní hospodářství | 2.1. | Zásobování pitnou a užitkovou vodou |
| | | 2.2. | Zabezpečení a správa povrchových vod z podzemních zdrojů vody |
| | | 2.3. | Systém odpadních vod |
| 3. | Potravinářství a zemědělství | 3.1. | Produkce potravin |
| | | 3.2. | Péče o potraviny |
| | | 3.3. | Zemědělská výroba |
| 4. | Zdravotnická péče | 4.1. | Přednemocniční neodkladná péče |
| | | 4.2. | Nemocniční péče |
| | | 4.3. | Ochrana veřejného zdraví |
| | | 4.4. | Výroba, skladování a distribuce léčiv a zdravotnických prostředků |
| 5. | Doprava | 5.1. | Silniční |
| | | 5.2. | Železniční |
| | | 5.3. | Letecká |
| | | 5.4. | Vnitrozemská vodní |
| 6. | Komunikační a informační systémy | 6.1. | Služby pevných telekomunikačních sítí |
| | | 6.2. | Služby mobilních telekomunikačních sítí |
| | | 6.3. | Radiová komunikace a navigace |
| | | 6.4. | Satelitní komunikace |
| | | 6.5. | Televizní a radiové vysílání |
| | | 6.6. | Poštovní a kurýrní služby |
| | | 6.7. | Přístup k internetu a datovým službám |
| 7. | Bankovní a finanční systém | 7.1. | Správa veřejných financí |
| | | 7.2. | Bankovnictví |
| | | 7.3. | Pojišťovnictví |
| | | 7.4. | Kapitálový trh |
| 8. | Nouzové služby | 8.1. | Hasičský záchranný sbor ČR a příslušné jednotky |
| | | 8.2. | Policie ČR (vnitřní bezpečnost a veřejný pořádek) |
| | | 8.3. | Armáda ČR (zabezpečení obrany) |
| | | 8.4. | Radiační monitorování včetně podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření |
| | | 8.5. | Předpovědní, varovná a hlásná služba |
| 9. | Veřejná správa | 9.1. | Státní správa a samospráva |
| | | 9.2. | Sociální ochrana a zaměstnanost (sociální zabezpečení, státní sociální podpora, sociální pomoc) |
| | | 9.3. | Výkon justice a vězeňství |

# 2 Prostředky pro využití v kritické infrastruktuře

V této kapitole jsou popsány jednotlivé technologie, které mohou najít využití ve zvyšování kritické infrastruktury nejen státu, ale i průmyslu a služeb. Vestavěné systémy představují hardwarový základ, M2M zařízení systém jejich komunikace a Internet of Things pak propojení těchto komunikačních prvků do větších funkčních struktur. Prostory pro ukládání velkého množství dat obstarávají cloudové služby. Infrastruktury vytvořené těmito technologiemi se budou rozkládat na velkých územních oblastech. Proto se jako ideálním řešením jeví využití komerčních mobilních sítí jako zprostředkovatele přístupu k těmto službám.

V České republice a ve světě se této problematice dostává vysoké pozornosti na odborných konferencích jako Embedded world, eHealth, Smart Factory, Smart Cities nebo IoT forum. Těchto konferencí se účastní přední výrobci telekomunikačních zařízení a IT jako jsou Microsoft, Intel, Cisco, což dokládá zájem o dané téma.

## 2.1 Vestavěné systémy

Podstatou Embedded systémů je zabudování řídícího sytému do zařízení. Tyto řídicí systémy jsou nakonfigurované pro přesné plnění konkrétního úkolu, a proto jsou často označovány jako jednoúčelové. To umožňuje výrobcům jednoduše optimalizovat chod toho zařízení pro danou aplikaci a snížit tak výrobní náklady. Software určený pro vestavěné systémy se nazývá firmware. Jelikož úroveň tohoto softwaru nedosahuje náročnosti operačních systémů osobních počítačů, pro jejich implementování do zařízení nejsou třeba klasické pevné disky, ale zařízení si vystačí s uložením dat do pamětí, jako jsou Flash a ROM. Mnohem větší nároky se kladou na spolehlivost a bezporuchovost. V tomto ohledu musí být vestavěné systémy vyvíjeny s větší pečlivostí než programy osobních počítačů. Zařízení totiž často neobsahují žádné nebo jen omezené vstupy jako je klávesnice či monitor pro opravu zařízení. Chybu tak nelze řešit postupy jako u standardní výpočetní techniky. V případě neočekávané chyby je často použit mechanismus resetování systému, takže zařízení je schopno se samo zotavit z poruchy.

Vestavěné systémy našly největší využití ve spotřební elektronice, jako jsou mp3 přehrávače, herní konzole, digitální fotoaparáty. Mezi další odvětví patří vestavěné spotřebiče jako lednička a mikrovlnná trouba. Kromě těchto jednoduchých aplikací jsou implementovány například v automobilovém průmyslu v podobě řídících jednotek nebo systémů jako ABS, kde vedly k významným technologickým pokrokům z hlediska spolehlivosti a bezpečnosti.

Technologický vývoj některých těchto zařízení, příkladem je mobilní telefon, vedl k neustálému zvyšování úrovně po hardwarové i softwarové stránce. Dnešní smartphony jsou vybaveny plnohodnotnými operačními systémy a jejich výpočetní výkon už se nijak diametrálně neodlišuje od výkonu osobních počítačů. Tento pokrok vedl k stírání rozdílů mezi vestavěnými a víceúčelovými systémy.

## 2.2 M2M

Zkratka M2M má v literatuře několik výkladů. Nejčastěji je prezentována pod výrazem Machine to Machine, tedy komunikace stroje se strojem, v některých případech Machine to Mobile. Tento typ komunikace se vyvinul z předchozího modelu M2H, Machine to Human, spojení mezi strojem a člověkem. Jak lze vyvodit z těchto výrazů, rozdíl mezi těmito spojení spočívá v nahrazení člověka jako účastníka komunikace jiným strojem. Tento základní model spočívá v komunikaci 2 zařízení mezi sebou prostřednictvím sítě jako komunikačního média. Myšlenkou tohoto modelu bylo vytvořit komunikaci velkého počtu zařízení mezi sebou bez zásahu člověka. Propojení těchto strojů je převážně bezdrátové. Tak lze dosáhnout automatizované komunikace mezi jedním či více zařízeními (například senzory) s centrálním řízením. Centrální zařízení tvoří základ pro výměnu informací.

Komunikace M2M se skládá ze tří kroků – sběru dat, přenosu dat a zpracování dat. Sběr dat představuje naměření hodnot senzory. Tyto data jsou poté přenesena do centrálního prvku. Sběr a přenos dat může být od senzorů vyžádán centrálním prvkem nebo k němu dochází za podmínek nastavených na senzorech, jako je určený časový interval či definované změně naměřených údajů. Zpracování dat v centrálním prvku spočívá v analýze a ukládání dat, případně i reakci centrálního prvku na zařízení.

K velkému nárůstu použití M2M v současné době napomohlo zavedení bezdrátových telekomunikačních technologií, které usnadňují přenos dat mezi zařízeními, ať už se jedná o přenos dat na malé vzdálenosti jako je Bluetooth, Wi-Fi či RFID (Radio Frequence Identification), nebo přenos na velké vzdálenosti prostřednictvím mobilních sítí**.**

Komunikace mezi zařízeními se tak stane zcela běžnou součástí, tak jako je komunikace lidí. S rostoucí přenosovou kapacitou sítí a dokonalejším pokrytím se zvýší flexibilita nasazení M2M technologií do dalších průmyslových i komerčních užití. M2M zařízení mají ve své architektuře několik vlastností, kterými se významně liší od jiných prvků, které je nutné brát v potaz při jejich případném využití:

- **Kvantita** – Množství M2M zařízení stále narůstá. Podle odhadů společnosti Ericsson, má v roce 2020 počet M2M zařízení dosáhnout 26 miliard [1], [10]**.** Počet M2M zařízení tak značně přesáhne počet zařízení, které obsluhuje člověk, mezi které patří osobní počítače, smartphony, tablety aj. Tento aspekt bude klást velké nároky na propustnost sítí z důvodu velkého vytížení těmito zařízeními. Dopad značného vzrůstu počtu připojených zařízení pocítí nejen poskytovatelé mobilních sítí, ale i systémy a provozy navržené pro správu malého počtu zařízení [10]. Tím značně vzrostou i nároky pro zachování či vylepšení stávajících kvalit služeb – QoS (Quality of Service).
- **Široké množství využití** – Již v současné době výrobci prezentují řadu možností využití M2M zařízení a v budoucnu se dá očekávat pokračování tohoto trendu. Stejně jako bude mít každé toto implementování odlišné výhody pro danou službu, budou se lišit i nároky a požadavky na jednotlivá M2M zařízení. Mezi tyto nároky patří potřebný výpočetní výkon, požadovaná rychlost přenosu a typ komunikace. Snaha výrobců bude dosáhnout co nejnižšího potřebného výpočetního výkonu z důvodů dosažení co nejmenších výrobních nákladů. Vzhledem k tomu bude obtížné zrealizovat technické či funkční aktualizace těchto zařízení. Rozdílné technické řešení M2M zařízení jednotlivých výrobců

bude mít za následek snahu prosazovat svoji verzi řešení této problematiky, takže bude obtížné tyto sítě testovat a vytvořit jednotný standard.

- **Správa** – Jak bylo popsáno v definici samotného modelu M2M komunikace, přenos, zpracování a analýza dat musí probíhat bez většího zásahu člověka. Z toho plynou vysoké nároky na spolehlivost těchto systémů, protože některé z nich není člověk bez potřebné kvalifikace kromě základní obsluhy více spravovat. Mnoho z nich je navíc zabudovanou součásti větších struktur, jako je řídící jednotka automobilu, a její výměna tak není možná bez většího zásahu do systému.
- **Nízká spotřeba** – Pokud je to možné, senzory jsou v rámci instalace napojeny na elektrickou rozvodnou síť. V některých případech venkovní použití, které jsou jen těžko přístupné, není napojení možné a senzory tak musí být napájeny akumulátory. Senzory jsou proto konstruovány na vhodných frekvencích, čímž lze životnost baterie prodloužit až na 10 let. Pokroky v oblasti v oblasti materiálů jako superkondezátory a mikrokontroléry mají v budoucnu vést k zařízením, které budou schopna dobíjet akumulátory přeměnou okolní energie na energii elektrickou [2]. Mezi tyto zdroje patří sluneční energie, radiové signály, rozdíly teplot.
- **Životnost** – Kromě životnosti baterie jsou kladeny vysoké nároky na celkovou životnost M2M zařízení. Zařízení budou totiž často zabudovaná do složitějších systémů a funkčních celků (například v automobilovém průmyslu jako součást motoru) a proto případná výměna bude velmi náročná.

### 2.2.1 Architektura sítí

Základní architektura spočívá v komunikaci 2 zařízení přes přenosové médium. V systému vestavěných zařízení tento model však zbytečně zatěžuje síť. Propojením, více zařízení dohromady vznikne síť následující architektury:

- **M2M zařízení (device)** – Zařízení nasazené uživatelem k zachycení událostí a dat.
- **M2M brána (gateway)** – Pomáhá propojit datové toky ze zařízení do propojovací sítě.
- **M2M lokální síť (local network)** – Skupina M2M zařízení a Gateway. Její výhodou je použití jedné brány pro více zařízení.
- **M2M propojovací síť (communication network)** – Zajišťuje komunikaci mezi M2M bránou a M2M aplikací. Příkladem propojovací sítě M2M je mobilní datová síť LTE

Na výstupu této komunikační sítě se nachází aplikační doména. Tu představuje uživatel, který data využívá, případně M2M aplikace, jejímž prostřednictvím uživatel dostává výstup dat.

### 2.2.2 Přehlcení sítě

Jelikož M2M zařízení pracují v ideálním případě bez zásahu člověka a stávají se tak „neviditelnými“ nemá uživatel takový přehled o míře komunikace jako u zařízení M2H. V důsledku toho může v sítích zařízení docházet k přetížení, které rozlišujeme podle příčiny vzniku:

- **Synchronizační** – Nejčastější způsob zasílání dat M2M zařízení probíhá v nastavených časových intervalech. V případě, že se v síti nachází více zařízení posílajících data ve stejnou dobu (například v každou celou hodinu) dochází tak v daný okamžik k jednorázovému přetížení sítě.
- **Nepředvídatelné –** Zařízení je do sítě nainstalováno bez vědomí poskytovatele. Poskytovatel nepočítá s nárůstem zatížení sítě a tak dochází k přehlcení.
- **Nárazové –** Určité druhy zařízení při své činnosti posílají za normálních podmínek pouze malé množství dat. Při změně těchto podmínek (například překročení dovolené hodnoty) dojde k prudkému nárůstu generovaných dat ze zařízení, což vede k přehlcení.

### 2.2.3 Bezpečnost zařízení

Spolehlivost výpočetní techniky je do jisté míry dána i úrovní zabezpečení. M2M zařízení jsou v tomto ohledu rizikovější z důvodu jejich neviditelnosti. Tu může představovat fyzická vzdálenost od centrálního řídícího prvku nebo charakter jejich komunikace, který probíhá v jejich vlastní režii a tak správce či uživatel nemusí tento útok vůbec zaznamenat, případně jej odhalit s velkým časovým zpožděním. Útočník tak může bez jeho vědomí zařízení ovládat, získávat z něj informace, případně zasílat adresátovi klamné informace. Pokud mají být M2M zařízení použita v kritické infrastruktuře je třeba těmto rizikům předcházet, protože vyřazení z funkce by mohlo mít fatální následky. Pro ochranu se používají prostředky běžně používané výpočetní techniky, jako je přístup do zařízení administrátorským jménem a heslem a užitím firewallu s definovanými pravidly filtrování příchozí a odchozí komunikace.

### 2.2.4 Bezpečnost komunikace

Kromě zabezpečení samotného zařízení je třeba brát v potaz i rizika spojené s přenosem informace. Přenášená data mohou být napadena na cestě od zdroje na cílové zařízení. Jejich komunikace může být napadena z důvodu odposlechu a získání dat útočníkem, odstavení spojení mezi zdrojem a cílem, nebo kompromitace přenášených informací. Bezpečnost komunikačního kanálu se liší podle typu komunikačního média. Data se přenáší veřejnou sítí Internet nebo po vlastním komunikačním kanále. Tyto soukromé kanály jsou zprostředkovány provozovateli M2M služeb, který zabezpečuje bezpečnost přenosu dat. Výhodou z hlediska bezpečnosti je nutnost fyzického přístupu útočníka k tomuto médiu. Přenos dat prostřednictvím internetu je zpravidla zabezpečen šifrováním. Šifrování nemá vliv na možnost útočníka zachytit data. V ideálním případě tyto data však není schopen rozšifrovat a získat tak žádané informace. Nevýhodou šifrování jsou nároky na výpočetní výkon.

Vniknutím do komunikační sítě se může útočník pokoušet vydávat za jedno z komunikujících zařízení. Identifikátorem jednotlivých zařízení je totiž IP adresa, která je snadno získatelná monitorováním datové komunikace dané sítě. Prostředkem proti tomu typu útoku je použití autorizačního klíče, který se skládá z veřejného a soukromého klíče.

Jak bylo zmíněno výše, dosažení bezpečnosti zařízení M2M je spjato s nároky na jeho výpočetní výkon. Výrobci těchto zařízení však z důvodu snížení výrobní ceny nepřikládají těmto nárokům v některých případech dostatečnou pozornost.

## 2.3 Internet of Things

V doslovném překladu „Internet věcí“, představuje svět vzájemně propojených zařízení, jejíž počet není omezen. Základní myšlenkou Internetu věcí je připojit všechna tato zařízení k internetu. Jednotlivé prvky IoT, označované jako smart zařízení, jsou složené z vestavěných systémů osazených senzory, jejíž chod bude řídit software a budou mít přístup na internet. Spojením těchto technologií tak vzroste důležitost role komunikace M2M a její efektivity. Všechna zařízení a systémy budou vyžadovat jednoduchou a spolehlivou komunikaci. Vývoj technologických materiálů a mobilních sítí jako zprostředkovatele jejich komunikace tyto nároky významně pomůže splnit. Tím se dosáhne propojení fyzického a kybernetického světa v novém měřítku.

V současné době se nedá říci, že by Internet věcí byl již fungující a zavedený systém. Tato technologie stále nese přízvisko budoucnosti. Že se nejedná o pouhé vizionářství, dokládají prognózy firem zabývajících se průzkumem trhu a plány výrobců, které směřují k roku 2020 [8]. Vzhledem k předpokládanému počtu zařízení, které budou do této doby k internetu připojena, nastane problém adresace těchto zařízení v síti. V současné chvíli používaný protokol IPv4 totiž neposkytuje dostatečný prostor pro takový počet zařízení. Jeho teoretická kapacita 4 miliardy jedinečných IP adres je šestinásobně menší, než předpokládaný počet zařízení. Adresa IPv6 se skládá ze 128 bitů oproti 32 bitové adrese protokolu IPv4, takže bude schopna pojmout $3{,}4\times10^{38}$ unikátních adres. Přechod na tento protokol zasáhne všechny síťové prvky, které s tímto protokolem nejsou kompatibilní. Technologie 5G a IPv6 budou tvořit základ pro vytvoření masivní sítě chytrých zařízení pracujících na úrovni komunikace M2M.

K zrealizování těchto plánů je ale třeba vyřešit problematiku jednotného standardu, na základě kterého budou zařízení komunikovat. Tendence výrobců je však vytvářet uzavřené systémy, nad jejichž vývojem a správou mají dokonalou kontrolu. Využití jednotného standardu pro široké spektrum zařízení zároveň přináší rizika spojená s bezpečností. Pokud se případnému útočníkovi podaří tyto standardy analyzovat, nalezne cestu jak na systémy zaútočit a vyřadit je tak z provozu [7].

Největší potenciál však nespočívá v samotných zařízeních, ale v datech, které produkují. Tyto informace, nazývané Big Data, je třeba odpovídajícím způsobem efektivně zpracovat, analyzovat a poté sdílet. V otázce sdílení se počítá v umístění dat do tzv. Cloudů, které umožní přístup k datům pomocí webového prohlížeče nebo k tomu určené aplikace Tento rozsáhlý proces zpracování dat umožní zefektivnit výrobní procesy průmyslových továren, ale i zvýšit životní úroveň a komfort běžných uživatelů.

Z výše zmíněné problematiky se dají shrnout základní požadavky na zařízení, které budou připojena do sítě internet:

- **Mít jedinečnou identitu –** prvek musí být adresovatelný a rozpoznatelný v rámci sítě.
- **Schopnost analýzy** – zařízení na základě výstupů z připojených senzorů snímajících danou veličinu musí být schopné tyto výstupy zpracovat a prezentovat formou stavů, atributů nebo dat.
- **Schopnost komunikace** – zpracované data

- **Schopnost interakce** – na základě rozhodnutí vyšších objektů či aplikací musí být zařízení schopno adaptivně měnit svůj stav či nastavení atributů.

### 2.3.1 Big Data

Připojením obrovského množství zařízení do internetu a jejich komunikací ať už s uživatelem či mezi sebou, přináší obrovské objemy dat, které nebude možné efektivně zachycovat, zpracovávat a analyzovat současně dostupnými metodami a aplikacemi. Problém toho nárůstu množství dat spočívá kromě objemu samotného v dalších 2 oblastech – různorodosti dat a rychlosti.

- Různorodost dat – Omezené množství druhů dat umožňuje jednoduché strukturování dat podle jejich charakteru a jejich centralizaci. Nástupem Internetu věcí do sítě vniknou nové typy zařízení, produkující nové typy dat či generaci dat ve zcela novém kontextu.
- Rychlost – Propojení senzorů generujících data k internetu umožňuje přenos těchto dat v reálném čase. Aby tento přenos měl smysl, bude potřeba tyto data umět v reálném čase také zpracovat a analyzovat.

Východiskem rychlosti dat je hledání a dosažení vyšších výpočetních výkonů serverů, která tato data budou zpracovávat. Jedná se především o zvýšení výkonosti procesorů, pamětí a nalezení nových způsobů zpracování dat jako jsou paralelní výpočty. Big Data otevřela prostor pro in-memory databáze. Jejich výhodou je ukládání velkých objemů dat přímo do paměti serveru. Ty dosahují mnohem vyšších rychlostí ukládání než nynější použití diskových polí. Data tak lze zpracovat v reálném čase a vytvářet tak výstupy pro uživatele.

### 2.3.2 Cloud computing

Potřeba neustále zvyšujícího množství ukládaných dat vedla k vytvoření nového modelu prostředí, kde jsou uložena. Cloud computing charakterizuje poskytnutí služeb a programů uložených na internetovém serveru. Důležitou vlastností této služby je možnost přístupu prakticky z jakéhokoliv místa. Přístup je umožněn širokému množství platforem klientských zařízení jako stolní počítače, notebooky, tablety či smartphony. pomocí specializované aplikace či webového prohlížeče bez nutnosti instalace softwaru. Poskytovatelé cloudových služeb kromě datových kapacit nabízí kancelářské aplikace, propůjčení výpočetního výkonu serverů až po operační systémy. Podle charakteru poskytovaných služeb rozlišujeme 3 základní modely Cloudů [9]:

- **Infrastructure as a Service (IaaS)** – Poskytovatel v tomto modelu vytváří klientovi infrastrukturu, která znamená vyčlenění hardwarových prostředků v podobě fyzických nebo virtuálních strojů. Veškeré záležitosti spojené s hardwarem garantuje a spravuje poskytovatel ze svého datového centra. Kromě výpočetního výkonu uživateli umožňuje umístění, škálování a zálohování jeho dat.
- **Platform as a Service (PaaS)** – Nabízenou službou je v tomto případě platforma, která zákazníkovi vytváří vývojové prostředí. Tím je obvykle samotný program, v němž celý vývoj aplikace probíhá. Tento program nabízí mnoho nástrojů pro správu a ladění

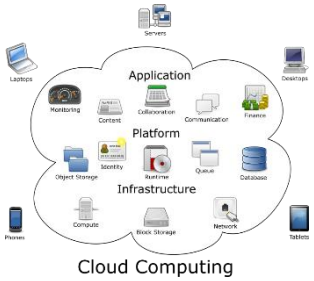
softwaru s cílem usnadnit práci programátora a zvýšit tak jeho produktivitu. Spotřebitel se tak může plně soustředit na vývoj a testování aplikace.

- **Software as a Service (SaaS)** – Poskytovanou službou se myslí pronájem softwarové aplikace uživateli. Uživatel tak nezískává software jako takový, je mu pouze umožněn přístup do této aplikace.

Kromě výše zmíněného modelu z hlediska poskytovaných služeb se cloudy rozlišují podle charakteru jejich infrastruktury na veřejné, soukromé, hybridní, komunitní a multicloudy.

- **Veřejný cloud (Public cloud computing)** – Klasický model cloudu, kdy je služba nabízena široké veřejnosti. Cloud může být v základním režimu zdarma a uživatel si může pronajmout další prémiové služby.
- **Soukromý cloud (Private cloud computing)** – Cloud je provozován výhradně pro jednu organizaci a to buď organizací samotnou, nebo třetí stranou.
- **Hybridní cloud (Hybrid cloud computing)** – Hybridní cloudy kombinují vlastnosti veřejných a soukromých cloudů. Navenek působí jako jeden cloud, ale ve skutečnosti se jedná o propojenou strukturu více cloudů. Nejčastější způsob spočívá rozdělení dat podle jejich citlivosti a určení kompetencí uživatelů. K základním datům mají přístup všichni zaměstnanci a firmy formou cloudu veřejného. Naopak k citlivým informacím uložených na soukromém cloudu se tak dostanou pouze určení uživatelé.
- **Komunitní cloud (Comunity cloud computing)** – Infrastruktura cloudu je sdílena ve společenství organizací, které ji využívají. Tyto organizace spojuje stejný obor zájmů.
- **Multicloud –** Důvodem pro zavedení multicloudové infrastruktury je snaha uživatele dosáhnout vyšší flexibility služeb vytvořením heterogenní architektury. Uživatel má tak k dispozici více samostatných dodavatelů cloudových služeb. Každý dodavatel může klientovi poskytovat jiný model služby (například první dodavatel IaaS, druhý SaaS) nebo naopak stejnou službu, čímž dojde k rozložení zátěže. Od hybridního cloudu odlišuje poskytováním více služeb jednomu klientovi, na rozdíl od hybridního poskytování jedné služby více klientům.

Jako jednou z klíčových vlastností IoT je považována interoperabilita. Té se má v souvislosti s cloudy dosáhnout vytvořením Intercloudu, který bude fungovat jako globální „mrak mraků“. Jedná se o nástavbu hybridního a komunitního cloudu, umožňující lepší kooperaci a flexibilitu cloudových systémů, k zlepšení kvality služeb pro klienta. Klient bude moci v reálném čase jednoduchými požadavky dosahovat navýšení či snížení výpočetního výkonu podle aktuální potřeby. Kooperace více společností (například při společných projektech) bude usnadněna sdílením služeb a dat mezi sebou, přestože každá ze společností bude náležet odlišné infrastruktuře.




Obrázek 2.1 Cloud Computing

# 3 Využití komerčních mobilních sítí

V této kapitole jsou uvedeny metody aplikované do mobilní sítí LTE pro zabudování technologií zmíněných v kapitole 2. Následují příklady aplikace tohoto spojení v některých odvětvích kritické infrastruktury a zároveň využití v průmyslu a službách.

## 3.1 LTE D2D

S výše zmíněnou komunikací strojů M2M a Internetem věcí IoT vznikly nové požadavky na vysokorychlostní mobilní sítě, od kterých se očekává, že převezmou hlavní podíl na zajištění komunikace M2M.

Systém LTE D2D (Device to Device), v některých případech též nazýván LTE-M je specifikován ve standartu LTE 3GPP (3rd Generation Partnership Project) Release 12 v části ProSe (Proximity Services). Definuje komunikaci M2M zařízení s nejbližším mobilním zařízením. Jedná se o typ komunikace peer-to-peer, která nevyužívá infrastrukturu mobilní sítě, ale umožňuje zařízením založených na LTE komunikovat přímo spolu navzájem, pokud jsou v těsné blízkosti. Připojením M2M zařízení do mobilní sítě LTE vznikají následující výhody a možnosti:

- **Přenosová rychlost** – Zařízení mohou být vzdálena od buňkové infrastruktury, a proto nemusí být schopna podporovat vysoké přenosové rychlosti, které od nich jsou požadovány. Přímá komunikace mezi blízkými zařízeními může dosáhnout vyšší propustnosti a nižší latence než komunikace přes LTE základnové stanice eNode B.
- **Spolehlivost komunikace** – LTE zařízení může být využito pro komunikaci s lokálními zařízeními, což poskytuje vysokou spolehlivost komunikace i v případě, kdy z jakéhokoliv důvodu selže sít LTE .
- **Naléhavá komunikace** – Vzhledem k tomu, že komunikace D2D není závislá na síťové infrastruktuře, zařízení může být použito pro komunikace s větším počtem zařízení způsobem, který je používán u vysílaček [20]. Tento aspekt může být zvlášť užitečný pro komunikaci záchranných složek [20].
- **Využívání licencovaného spektra** – Na rozdíl od zařízení pracujících v nelicencovaných frekvenčních pásmech, jako je WiFi ( Wireless Fidelity) či Bluetooth, budou LTE zařízení používat licencované spektrum, které je méně náchylné k interferencím, a tím umožní spolehlivější komunikaci [20].
- **Redukce rušení** – Tím, že komunikace probíhá přímo mezi zařízeními bez použití základnové stanice, je ve frekvenčním spektru přenášeno méně dat. Je tak dosaženo větší účinnosti než za použití buněk malé velikosti [20].
- **Úspora energie** – Krátká vzdálenost mezi vysílačem a přijímačem poskytuje lepší podmínky pro propojení, a tedy účinnější spojení s nižší spotřebou energie.

Přepínání mezi komunikací v buňce a přímými komunikačními M2M módy slouží především k optimalizaci výkonu přístupové sítě. Silnou stránkou tohoto řešení je, že mobilní síť využívá výhod M2M komunikace, bez výrazného vlivu na zatížení sítě, zatímco pro koncového uživatele jsou tyto změny přenosu zcela transparentní. Problémem tohoto řešení je zabránit přerušení spojení přepínáním z jednoho režimu do druhého.

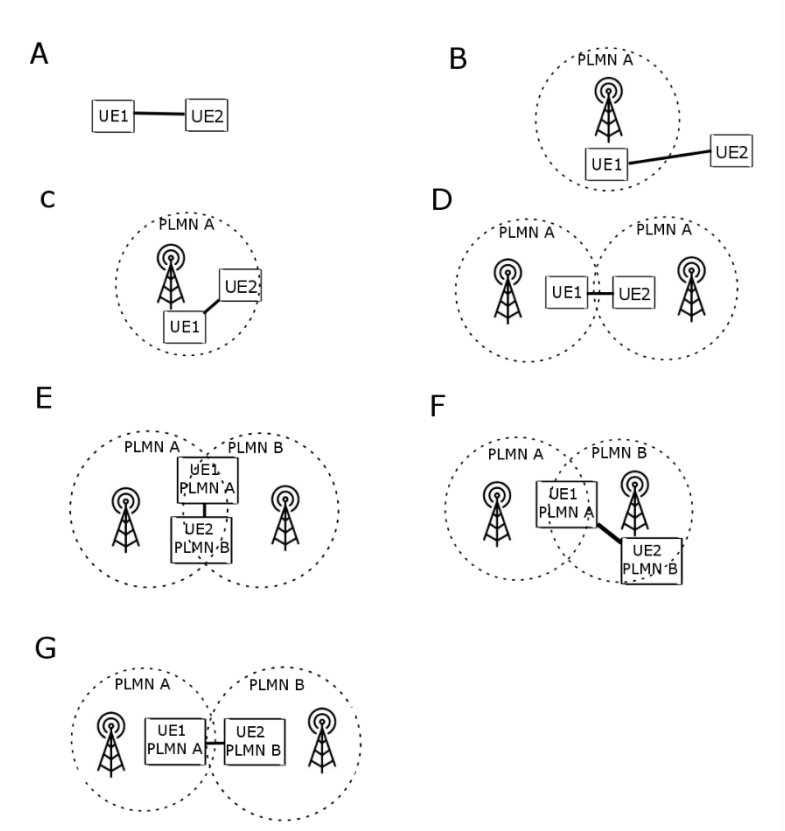
Dalším možným přístupem je návrh na změnu síťové architektury LTE, která má za cíl nabídnout pro M2M komunikaci sdílení či přidělení prázdných částí spektra nezávisle na přenosech v buňce. Tímto přístupem vznikne přímé spojení s páteřní sítí, která zvládne obsluhovat oba typy komunikace samostatně.

Připojení M2M zařízení do mobilní sítě LTE spolu s možností přímé komunikace vytváří zcela nové scénáře situací, které mohu mezi jednotlivými prvky nastat. Tyto scénáře pro případ dvou zařízení jsou shrnuty v tabulce **Chyba! Nenalezen zdroj odkazů.** a na obrázku 3.1.

Na obrázku 3.1 je uveden pojem PLMN, který označuje veřejný identifikátor sítě a skládá se z MCC (Mobile Country Code) a MNC (Mobile Network Code). MCC je identifikátor mobilního operátora v měřítku dané země. Všichni operátoři působící na území jednoho státu mají přidělený stejný MCC. Operátoři jsou od sebe odlišeni pomocí identifikátoru sítě (MNC).

Tabulka 3.1 Scénáře komunikace M2M v mobilní síti

| Scénář | Pokrytí buňkou 1 | | Pokrytí buňkou 2 | | Podřízenost UE 1 | | Podřízenost UE 2 | |
|---|---|---|---|---|---|---|---|---|
| | UE1 | UE2 | UE1 | UE2 | PLMN A | PLMN B | PLMN A | PLMN B |
| A | NE | NE | NE | NE | NE | NE | NE | NE |
| B | ANO | NE | NE | NE | ANO | NE | NE | NE |
| C | ANO | ANO | NE | NE | ANO | NE | ANO | NE |
| D | ANO | NE | NE | ANO | ANO | NE | ANO | NE |
| E | ANO | ANO | ANO | ANO | ANO | NE | NE | ANO |
| F | ANO | NE | ANO | ANO | ANO | NE | NE | ANO |
| G | ANO | NE | NE | ANO | ANO | NE | NE | ANO |




Obrázek 3.1 Scénáře komunikace M2M v mobilní síti

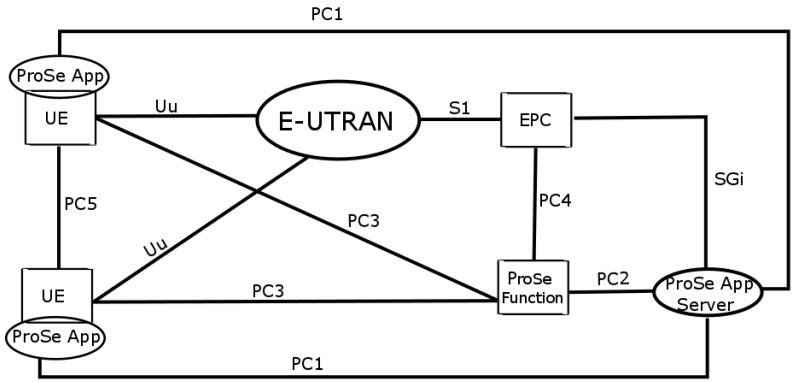
Popis jednotlivých scénářů:

- **A** – 2 mobilní terminály spolu komunikují v přímém režimu bez použití standardní infrastruktury LTE.
- **B** – UE1 spadá fyzicky i strukturně pod operátora A. UE2 se nachází mimo síťovou infrastrukturu. Komunikace tak bude probíhat stejně jako v případě A v přímém režimu-
- **C** – Oba terminály se nachází v buňce svého operátora.
- **D** – UE se fyzicky nachází v odlišných buňkách svého domácího operátora.
- **E** – Terminály odlišných operátorů jsou fyzicky umístěny v současném pokrytí domovského a cizího operátora.
- **F** – UE1 se fyzicky nalézá na rozhraní buněk obou operátorů. UE2 je umístěn pod pokrytím svého domovského operátora.
- **G** – Terminály odlišných operátorů se fyzicky nachází v různých buňkách patřících domovským operátorům.

Ve scénářích C až G je možná komunikace jak v přímém režimu, tak přes eNode B daného operátora. V těchto případech bude třeba vyřešit algoritmy, podle kterých se UE rozhodnou pro daný typ přenosu. S nárůstem komunikujících zařízení se počet možný scénářů zvyšuje.

Pro funkci výše znázorněných scénářů je nutné vylepšení LTE architektury. Obrázek 3.2 znázorňuje modifikovanou architekturu LTE po implementaci služeb ProSe, která má za cíl splnit následující požadavky:

- Umožnit operátorovi řídit funkce ProSe discovery ve své síti a stanovit požadavky rozpoznávacích funkcí každého UE.
- Povolit autorizovaným aplikacím třetí strany přístup do infrastruktury k využití ProSe služeb nabízených v dané síti.
- Ovládat komunikaci mezi UE a ProSe spadajících pod stejnou nebo rozdílnou eNode B.
- Přizpůsobit funkce ProSe z hlediska bezpečnosti komunikace a ochrany soukromí.
- Umožnit operátorovi autorizaci a autentizaci aplikací třetí strany před využitím ProSe.




Obrázek 3.2 Zjednodušená architektura LTE po zabudování ProSe

Jak vyplývá z obrázku 3.2, kromě standartních prvků LTE architektury jako je uživatelské zařízení, přístupová síť E-UTRAN (evolved UMTS Terrestrial Radio Access) a páteřní síť EPC (Evolved Packet Core) obsahuje schéma řadu nových prvků:

- **Aplikační server (ProSe App Server)** – představuje funkce pro specifické aplikace, například centra tísňového volání. Tyto aplikace jsou definovány mimo architekturu 3GPP. Aplikační server může komunikovat s aplikací v UE.
- **Aplikace v UE (ProSe UEs App)** – zajišťuje funkce ProSe na straně uživatele. Příkladem může být komunikace mezi příslušníky záchranných složek.
- **Funkce ProSe (ProSe Function)** – Referenční bod mezi UE, aplikačním serverem a páteřní sítí [19]. Úkolem referenčního bodu může být autorizace a konfigurace UE pro přímou komunikaci.

Kromě těchto nových prvků byla definována i nová rozhraní. Rozhraní mezi dvěma účastnickými terminály, PC5, je komunikační rozhraní one-to-many, které je určeno pro skupinovou komunikaci. Rozhraní PC3 slouží k propojení UE a referenčního bodu ProSe [19]. V Release 12 je pro jednu síť PLMN definován pouze jeden referenční bod. Rozhraní PC1 spojuje aplikaci v UE a aplikační server. Komunikace mezi referenčním bodem a páteřní sítí je definována jako rozhraní PC4.

Standard LTE D2D se stále nachází ve fázi výzkumu a vývoje. Před aplikací standardu do mobilních sítí je třeba vyřešit některé důležité otázky jako je přesný algoritmus pro přepínání mezi přímou komunikací a komunikací s eNode B, proces autorizace a autentizace, který má v současné době na starosti páteřní síť.

## 3.2 Energetika

Energetika je nejzranitelnějším prvkem kritické infrastruktury. Na jejím fungování jsou zcela závislé ostatní prvky kritické infrastruktury. Vyřazením produkce a dodávky energetických společností zcela zkolabují základní prostředky pro život, jako je dodávka vody, přepravní síť, zdravotnická péče a další nouzové služby.

Energetické systémy ohrožují havárie kritických prvků, způsobené nedostatečnou údržbou, selhání řídicího systému, teroristického útoku či živelné pohromy přírodního charakteru.

Nejvýznamnější oblastí energetiky je dodávky elektrické energie. Její značnou nevýhodou je téměř nulová možnost jejího uskladnění. Další komplikace způsobují především obnovitelné zdroje elektrické energie, jako jsou větrné a sluneční elektrárny, u kterých nelze odhadnout množství generované energie, protože jsou přímo závislé na přírodních jevech. Je proto třeba vytvořit účinné nástroje, které by umožnily výrobní a distribuční soustavu elektrické energie efektivně řídit.

Z hlediska informačních technologií je proto věnována značná pozornost využití tzv. „Inteligentní sítí“ (smart grids), které dopomohou vytvořit účinnou infrastrukturu. Vytvoření smart grids dosáhneme pokrytím napájecích sítí komunikační infrastrukturou. Základem těchto sítí je použití digitálních zařízení pro sběr dat. Vložením měřících prvků do klíčových míst sítě se vytvoří prostředky pro obousměrnou komunikaci. Tyto objekty budou vzájemně komunikovat prostřednictvím automatizovaného řídicího systému. Řídicí systém má za úkol dodávat vyprodukovanou energii podle aktuálních energetických nároků sítě.

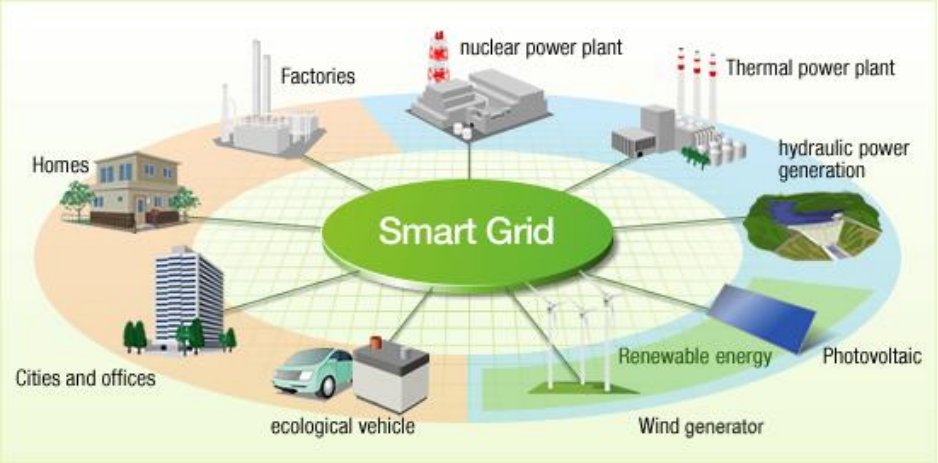
Zdigitalizováním naměřených dat získá poskytovatel okamžitý přehled o stavu o odběrných místech a může tak okamžitě reagovat na případná přetížení. Použitím chytrých měřidel není nutné provádět fyzický odečet spotřebované energie, protože tyto data je možné získat vzdáleným přístupem.

### 3.2.1 Požadavky na domácí automatizované systémy

- **Otevřenost a dostupnost** – Oproti uzavřeným systémům dosahují otevřené standardy faktory pro rychlejší rozvoj technologii na komerční trh. Otevřenost standardu umožňuje snazší interoperabilitu, multiple sourcing a snížení cenové politiky.
- **Rozsah** – Neboli pokrytí je jedním z nejdůležitějších požadavků na PLT.
- **Spotřeba** – Spotřeba energie je důležitý parametr pro kontrolu a řízení aplikací. Tento parametr je obzvlášť důležitý pro systémy napájené bateriemi. Vysoká spotřeba energie předpokládá větší napájecí zdroj, což vede k vyšším nákladům.
- **Přenosová rychlost** – V případě domácích automatizovaných systémů není přenosová rychlost klíčovým požadavkem. Rychlost přenosu dat 10 kb/s je v základních aplikacích, jako je například osvětlení, dostatečná pro použití v domácnostech. Kromě samotných dat je třeba počítat s použitím mechanismů pro dosáhnutí spolehlivého spojení, jako jsou směrovací protokoly, zabezpečení přenášených dat nebo přístupové mechanismy pro spojení s připojeným uzlem. S rostoucím počtem takto připojených sdělovacích uzlů v domácnostech se však

zvyšuje komunikační tok a zatížení. Proto by standard měl umožňovat variabilní datový tok k prevenci přetížení.

- **EMC** – Standard musí být v souladu s evropskými předpisy EMC platných v použitém kmitočtovém pásmu.
- **Bezpečnost** – Standard by měl poskytovat mechanismy na podporu šifrování a bezpečné datové služby. Zároveň by však měl být vhodným kompromisem mezi bezpečnostními nároky a náklady na jejich realizaci.
- **Latence** – Standard by měl umožňovat nízkou latenci komunikace s koncovým uživatelem, podle očekávání domácího použití. Zpoždění 200 ms je obvykle považováno za přijatelné maximum pro domácí automatizované systémy.




Obrázek 3.3 Decentralizovaná struktura Smart Grid

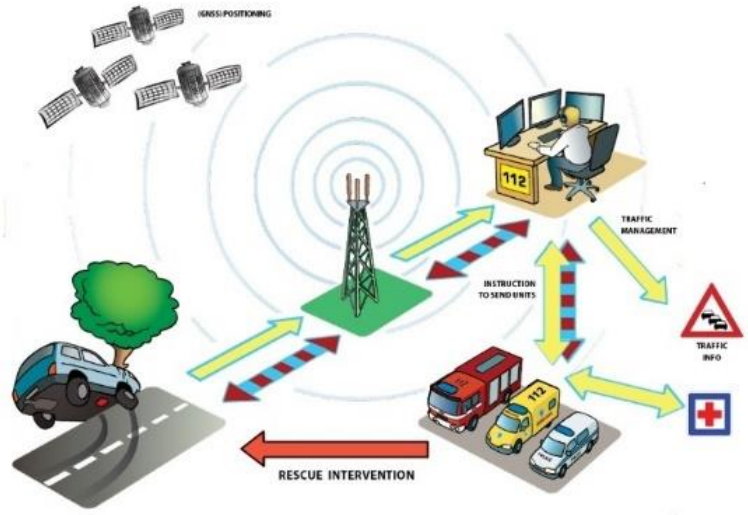
## 3.3 Zdravotnictví

Zdravotnictví je zcela specifická oblast pro zavádění informačních technologií. Z jedné strany její inovace a zlepšení služeb může mít zcela zásadní přínos pro lidstvo. Význam zdravotní péče nelze podcenit nejen z hlediska fungování státu. Člověk bez zdravotních problémů dosahuje vyšší životní úrovně a je produktivní. Na druhou stranu implementace nových technologií nese určitá rizika, která musí být zohledněny při jejich vývoji. Před skutečným uvedením do provozu musí být jakékoliv postupy či technologie důkladně propracovány a otestovány. Jejich špatná funkce či kompletní vyřazení z provozu by totiž bezprostředně mohlo vést k zhoršení stavu či smrti pacienta. Bezpečnost pacienta v těchto řešeních musí být bezpodmínečně na prvním místě.

Prostředky implementace technologií a jejich používání zdravotnictví se zabývá biomedicínské inženýrství. Ve spojení informatiky a zdravotnictví je častým pojmem bioinformatika. Bioinformatika je vědní disciplína, která se zabývá metodami sběru, shromažďování a analýzou biologických dat. Pro tyto účely se jeví jako ideální použití moderních senzorů. Senzory tak budou moci v reálném čase monitorovat základní lidské funkce. Již v dnešní době senzory umožňují monitorování aktivity člověka a životních funkcí jako je srdeční tep a tlak. V případě překročení povolených hodnot tyto senzory vyšlou informace uživateli, například do jeho mobilního telefonu. K této komunikaci je možné použít již fungující spojení technologií

krátkého dosahu jako je například Bluetooth. Prostřednictvím mobilní aplikace budou tyto data. Pacient tak dostane upozornění a včasným podáním příslušného léku může zabránit zhoršení svého zdravotního stavu. V ten samý okamžik budou tyto data odeslány mobilní datovou sítí do informačního systému a vloženy do karty pacienta. Změny těchto dat bude moci lékař analyzovat a upravit tak léčbu. V případě ohrožení života tento senzor zadá pokyn k okamžitému přivolání pomoci se zasláním polohy pomocí GPS modulu. Protože tento senzor bude jednoznačně identifikovatelný, bude snadné tak poskytnout informace o pacientovi přijíždějící záchranné službě [3]. Tak se dosáhne zefektivnění poskytnuté první pomoci a rychlému zásahu.

O interoperabilitě v Internetu věcí svědčí i následující příklad, který je popsán na obrázku. Při dopravní nehodě se závažnějšími poranění jsou klíčovými faktory včasný příjezd záchranných složek. Automobil prostřednictvím čidel zaznamená nehodu. V tu chvíli automaticky vyšle volání o pomoc, které bude zaznamenáno na centrále záchranných služeb. Ta k místu nehody vyšle složky Integrovaného záchranného systému. Díky sběru dat o dopravní situaci bude vyhodnocena nejrychlejší cesta k místu nehody a vozidlo záchranné služby se tak nedostane do žádné dopravní komplikace. Úspora tohoto času může být klíčovým rozdílem mezi životem a smrtí pacienta.




Obrázek 3.4 Modelová situace použití IoT ve zdravotnictví

## 3.4 Průmysl a služby

Průmyslové odvětví a výroba jsou klíčové oblasti, kde již nyní pozorujeme vliv Internetu věcí. Monitorování a údržba se staly nejběžnějším použitím Internetu věcí v průmyslovém světě. V oblasti výroby znamená propojení zařízení především zvýšení flexibility a produktivity. Výměna dat mezi stroji a systémy umožňuje pružně přizpůsobit řízení výrobku podle aktuálních požadavků.

Podniky tak mohou výrobní procesy lépe přizpůsobit stavu zakázek, aby kapacity a zdroje, které jsou k dispozici, byly optimálně využity. Sledováním strojů lze dosáhnout velké úspory na straně nákladů, a mimo jiné také zvýšit bezpečnost pracovníků na pracovišti. Velkou

příležitost vytváří internet věcí také v případě nakládání s produkty společností. Přidání konektivity k jejich produktům, umožňuje společnostem zvýšit hodnotu a funkce těchto produktů. Internet věcí se také stává velmi důležitou konkurenční výhodou pro udržení kontinuálního vztahu se zákazníkem.

## 3.5 Doprava

Dopravní prostředky jsou v dnešní době nezbytným aspektem pro život člověka. Vzhledem k rozloze infrastruktury měst a samotných států použití dopravních prostředků umožňuje přístup člověka k žádaným službám.

V současné době se zvyšuje počet automatizovaných zařízení, která umožňují monitorovat stav a údržbu automobilu a zvyšují tak bezpečnost a komfort řidiče. Vedle již zavedených zařízení jako je řídící jednotka či systém ABS zavádí automobilky pokročilé systémy, jakými jsou automatická asistence brždění, snímání sítnice řidiče, které snímají pozornost řidiče a upozorňují jej na případné riziko mikrospánku.

Standartní výbavou moderních automobilů se stal palubní počítač. Jeho prostřednictvím je řidič jednoduše schopen nastavit služby jako teplota v automobilu, vyhřívání sedaček, obsluha autorádia či zadání plánované trasy do GPS modulu. Tyto moduly používají data nahraná výrobcem k stanovení optimální trasy. Tyto data však postupem času nejsou aktuální. Připojením automobilů do Internetu věcí budou tyto automobily schopné nabízet aktuální informace v reálném čase, které získá z informačního systému monitorujícího dopravní situaci prostřednictvím semaforů, kamer i okolních aut. Řidič tak bude například upozorněn, že na plánované trase se stala dopravní nehoda a palubní počítač mu tak okamžitě nabídne alternativní trasy. Snímáním funkčních prvků bude dále schopný reagovat na poruchy a navést řidiče do nejbližšího servisu. Tato data zároveň poslouží výrobci automobilu k analýze nejčastějších závad daného modelu.

## 3.6 Chytré domácnosti

Výrobci informačních technologií jsou si dobře vědomy faktu, že pro rozšíření svých výrobků je třeba nalákat zákazníka prezentováním užitečnosti svého výrobku pro běžnou potřebu. Tento trend dokládá fakt, že jedním z prvních odvětví implementace chytrých zařízení byly zvoleny chytré spotřebiče do domácností. Propojením těchto spotřebičů v jeden funkční celek vznikají tzv. „Chytré domácnosti“. Tato zařízení mají za úkol zvýšit komfort jejich uživatele.

Jako další můžeme zmínit soubor zařízení, jejichž ovládání na dálku nebo schopnost rozhodovat se na základě dostupných informací přijde často velmi vhod. Může se jednat o systémy pro zavlažování, které mohou reagovat na podnět od uživatele nebo na vývoj počasí. Pak tu jsou další vhodné systémy, určené třeba pro ovládání topení/klimatizace a ohřev vody, sledování činnosti kolektorů, atd.

# 4 Využití mobilní sítě při mimořádných událostech

Podle zákona č. 240/2000 Sb., krizového zákona, ve znění pozdějších předpisů, lze stav nebezpečí vyhlásit v případě živelní pohromy, ekologické nebo průmyslové havárie, nehody nebo jiného nebezpečí, při němž jsou ohroženy životy, zdraví, majetek nebo životní prostředí, kde intenzita ohrožení sice nedosahuje značného rozsahu, ale není možné jej odvrátit běžnou činností správních úřadů a složek integrovaného záchranného systému.

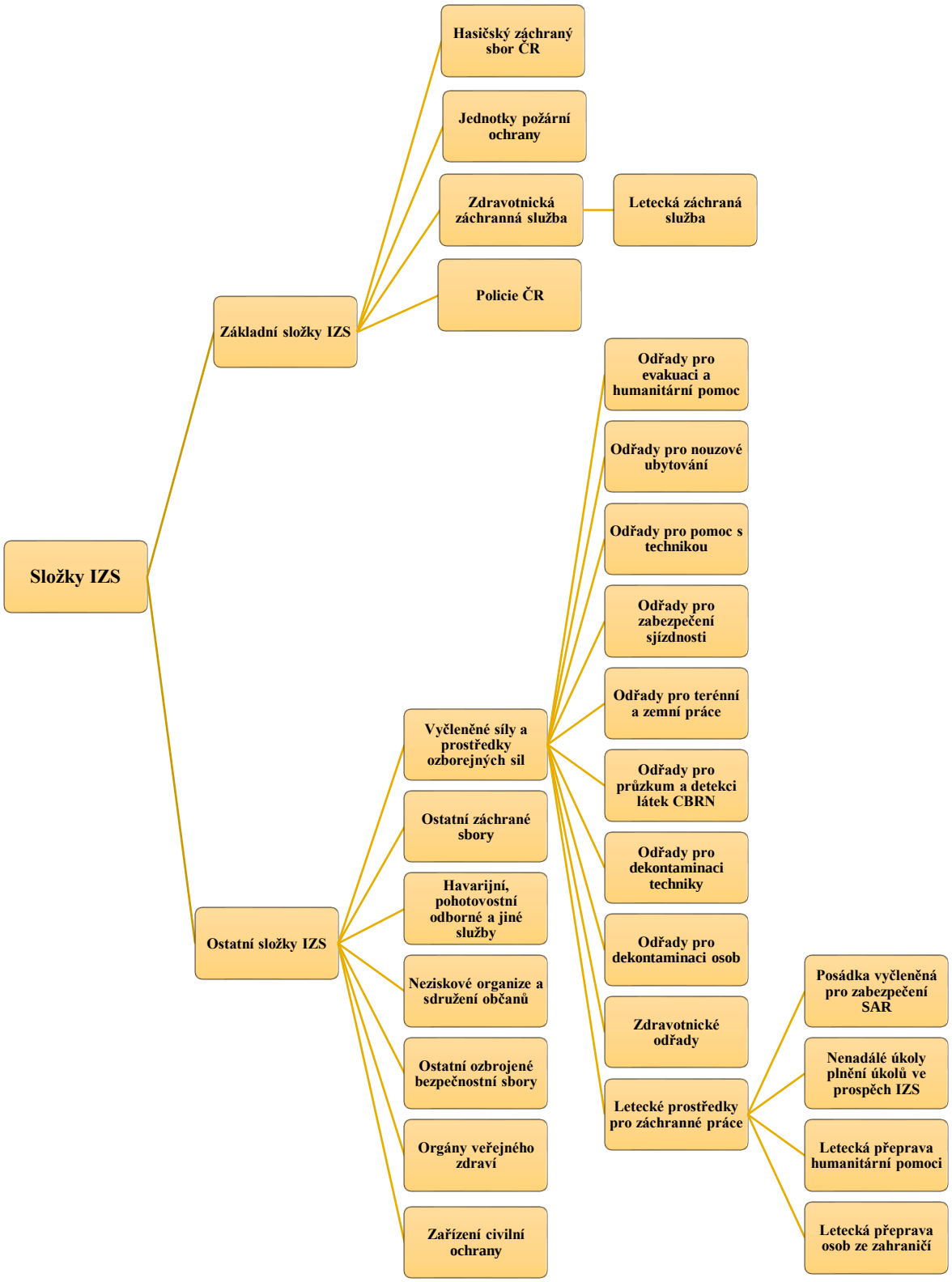
Stav nebezpečí je nejnižším z krizových stavů, který mohou orgány ČR vyhlásit v reakci na mimořádnou událost, závažnějšími stavy jsou nouzový stav a stav ohrožení státu. Vyhlašují ho hejtmani příslušných krajů, v případě Prahy její primátor. Musí být uvedeny důvody, území, pro něž je stav vyhlášen, krizová opatření a jejich rozsah. Vyhlašuje se nejvýše po dobu 30 dnů a tuto dobu může hejtman prodloužit jen se souhlasem vlády.

## 4.1 Integrovaný záchranný systém

Integrovaný záchranný systém (IZS) koordinuje postup jeho složek při přípravě na mimořádné události a při provádění záchranných a likvidačních prací. Jeho struktura se dělí na základní složky a ostatní složky a je znázorněna na obrázku 4.1.

Základní složky IZS jsou tvořeny Hasičským záchranným sborem ČR (HZS ČR), jednotkami požární ochrany, zdravotní záchrannou službou a Policií ČR. Mezi ostatní složky IZS patří vyčleněné síly a prostředky ozbrojených sil, ostatní ozbrojené bezpečnostní sbory, ostatní záchranné sbory, orgány ochrany veřejného zdraví, havarijní, pohotovostní, odborné a jiné služby, zařízení civilní ochrany, neziskové organizace a sdružení občanů, která lze využít k záchranným a likvidačním pracím. Ostatní složky integrovaného záchranného systému poskytují při záchranných a likvidačních pracích plánovanou pomoc na vyžádání.

Stálými orgány pro koordinaci složek integrovaného záchranného sboru jsou operační a informační střediska integrovaného záchranného systému. Těmito středisky jsou operační střediska hasičského záchranného sboru kraje a operační a informační středisko generálního ředitelství hasičského záchranného sboru.




Obrázek 4.1 Struktura integrovaného záchranného systému

## 4.2 Tísňové volání

Tísňové volání je základním způsobem ohlášení mimořádné události, při které je ohrožen život, zdraví, soukromý a veřejný majetek či životní prostředí. Tento prostředek má možnost využít každý občan k zajištění ochrany základních lidských práv. Účelem tohoto volání je vyžádání pomoci některé ze složek Integrovaného záchranného systému. Základní charakteristikou těchto linek je přednostní volání na tyto linky přiřazením vyšší priority volání ze stran mobilních operátorů. Všechny tísňové linky jsou bezplatné na základě číslovacího plánu vydaného Českým telekomunikačním úřadem [5]. Volání na tísňové linky lze uskutečnit i mobilním telefonem bez sim karty. V České republice je vyhrazeno 5 telefonních čísel pro tísňová volání:

- 112 – Jednotné evropské číslo pro tísňové volání
- 150 – Hasičský záchranný sbor ČR
- 155 – Zdravotnická záchranná služba
- 156 – Městská Policie
- 158 – Policie ČR

Na tyto čísla je garantovaný nepřetržitý přístup z pevných telefonních linek, mobilních telefonů i veřejných telefonních automatů. Poskytovatelé telefonních služeb mají tento přístup nařízen ze zákona. Jednotné evropské číslo pro tísňové volání bylo zavedeno rozhodnutím Rady Evropské unie z důvodu vytvoření univerzálního tísňového čísla pro všechny státy Evropské unie. Dosavadní národní čísla si jednotlivé státy mohly ponechat podle vlastního rozhodnutí. V České republice byl pro příjem volání na linku 112 určen nařízením vlády Hasičský záchranný sbor. Pro tento příjem bylo v krajských sídlech hasičských záchranných sborů vybudováno 14 telefonních center, která jsou vzájemně hlasově a datově propojená. V případě přetížení centra jsou tato volání přesměrována, čímž je docílena vzájemná zastupitelnost těchto center.

Zneužití tísňových linek za jiným než výše definovaným účelem se nazývá zlomyslné volání. Touto činností uživatelé blokují kapacity těchto linek nebo zapříčiní výjezd záchranných jednotek k fiktivní události. Vědomé zneužití tísňové linky je klasifikováno jako trestný čin, který může vést k vymáhání finančních sankcí, škody způsobené volajícím, případně zablokováním telefonního čísla. Český telekomunikační úřad může za takové volání uložit pokutu ve výši 100 000 Kč.

## 4.3 TETRA

TETRA (TErrestrial Trunked RAdio) je standardem pro trunkové (svazkové) radiové sítě. Standard byl definován evropským standardizačním institutem ETSI (European Telecommunications Standards Institute). Systém TETRA byl vyvinut pro komunikaci vládních úřadů, bezpečnostních a záchranných složek (záchranná služba, policie, armáda, hasičské sbory). Standard podporuje hlasové služby, komutovaná data a paketové datové služby s možnosti nastavení přenosové rychlosti a stupně zabezpečení dat. V roce 2005 byl vydán modernizovaný standard s názvem TETRA Release 2 označovaný rovněž jako TEDS (TETRA Enhanced Data Service), díky kterému došlo k nárůstu maximálního dosahu v režimu TMO (Trunked Mode Operation) z 58 km na 83 km [14].

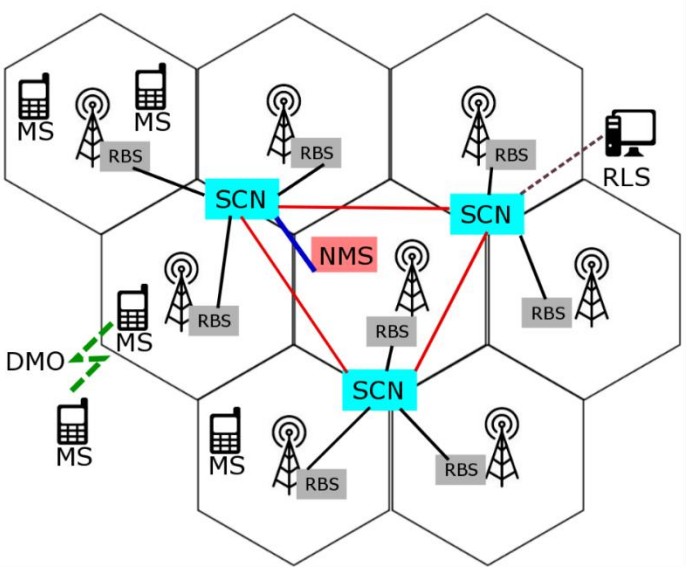
### 4.3.1 Charakteristiky systému

Systém TETRA byl od počátku vyvíjen jako celoevropský, proto bylo třeba vyhradit vhodná kmitočtová pásma, která splňují podmínky pro mezinárodní koordinaci. Pro záchranné služby (TETRA Emergency), byly vyčleněny frekvence 380-383 MHz a 390-393 MHz. Pro civilní sektor jsou pak v Evropě vyhrazena pásma 385-390 MHz, 395-399,9 MHz, 410-430 MHz, 450-470 MHz, 870-876 MHz, 915-921 MHz [14].

Za hlavní výhodu svazkových sítí je považována vysoká spektrální účinnost. Konvenční radiové systémy používají vyhrazený kanál pro každou jednotlivou skupinu uživatelů, zatímco trunkové sítě používají rozsah kanálů, které jsou dostupné pro různé skupiny uživatelů. Svazkové sítě tak umožňují sdílení relativně malého počtu frekvenčních kanálů mezi velké množství uživatelů. Vychází se z předpokladu, že celá skupina uživatelů nepotřebuje přístup ke kanálu ve stejný okamžik. Dostupné kanály jsou tak dynamicky přidělovány řídícím kanálem podle potřeby, což umožňuje použití menšího počtu kanálů. Pro zachování výhody jednoduchého sestavení hovoru slouží na terminálu radiostanice tlačítko PTT (Push To Talk). Po stisku tlačítka je hovor sestaven ve velmi rychlém čase, v průměru do 300 ms [16].

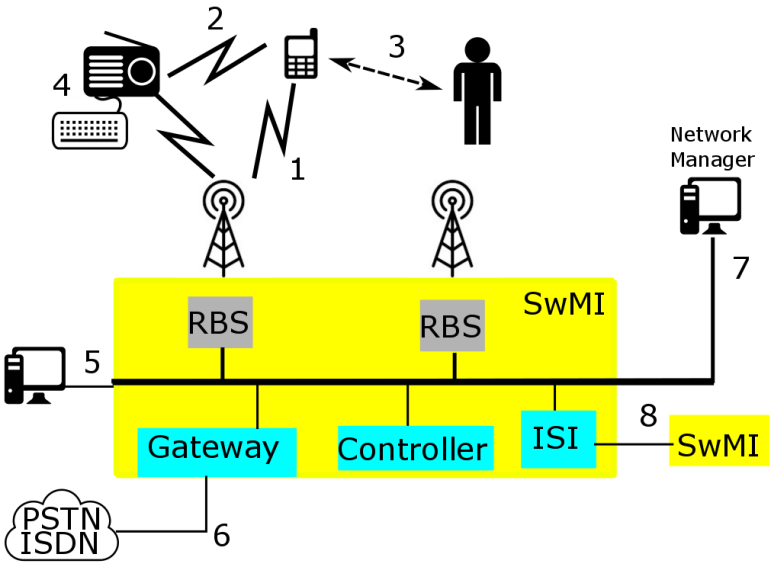
TETRA má obdobnou buňkovou architekturu jako telefonní GSM sítě. Základními síťovými prvky jsou:

- **MS (Mobile station)** – mobilní radiostanice, jedná se o přenosné a vozidlové radiostanice.
- **RBS (Radio Base Station)** – základnová radiostanice
- **SCN (Switching Controller Node)** – základnová řídící jednotka
- **NMS (Network Managment System)** – systém řízení sítě. Je zde uložena databáze uživatelů. Zabezpečuje řízení a dohled sítě.
- **RLS (Remote Line Station)** – centrální řídící prvek sítě, umožňuje komunikaci mobilních terminálů s dispečerem.




Obrázek 4.2 Architektura Systému TETRA

Na obrázku 4.2 jsou znázorněny 2 provozní režimy, ve kterých se může mobilní stanice nacházet. Provozní režim TMO je stav, kdy je stanice zaregistrovaná do síťové infrastruktury a komunikuje s ostatními terminály prostřednictvím základnové stanice. Režim, při kterém radiostanice komunikují mezi sebou bez použití základnové radiostanice se nazývá DMO viz kapitola 4.3.2. V režimu TMO probíhá provoz mezi rozhraními pomocí přepínání a řízení infrastruktury SwMI (Switching and Management Infrastructure). Jednotlivá rozhraní jsou znázorněna na obrázku 4.3:




Obrázek 4.3 Rozhraní TETRA

**Rádiové rozhraní (Air Interfaces)**

Jedná se o nejdůležitější rozhraní. Toto rozhraní představuje spojení mezi základnovou radiostanicí a radiovým terminálem (rozhraní č. 1), nebo rozhraní mezi radiovými stanicemi pracujícími v přímém operačním režimu DMO nezávisle na infrastruktuře sítě (rozhraní č. 2).

**Uživatelské rozhraní (Man-Machine Interface)**

Uživatelské rozhraní (č. 3) zpracovává vstupy uživatele, kterými uživatel radiostanici ovládá. Výstup uživatelského rozhraní prezentuje obsluze výsledky na základě zadaných vstupů.

**Rozhraní periferních zařízení (Peripheral Equipment Interface)**

Toto rozhraní standardizuje spojení radiové stanice a extérního zařízení (č. 4). Podporuje přenos dat mezi aplikacemi připojeného zařízení a radiovým terminálem TETRA.

**Dispečerské rozhraní (Local Dispatcher)**

Dispečerské rozhraní (č. 5) bylo původně zamyšleno k vzdálenému přístupu k dispečerským konzolím, které se nacházejí v kontrolních místnostech a velínech [17]. Stanovení jednotného rozhraní by však v tomto případě mohlo vést ke snížení výkonu sítě. Způsob připojení dispečerské aplikace do infrastruktury sítě závisí na požadavcích konkrétní aplikace.

**Rozhraní pro vnější sítě (Gateway for external networks)**

Toto rozhraní slouží k propojení veřejné telefonní sítě (Public switched telephone network) nebo sítě digitálních integrovaných služeb ISDN (Integrated Services Digital Network) k infrastruktuře sítě TETRA [17].

**Vnitřní systémové rozhraní (Inter System Interface)**

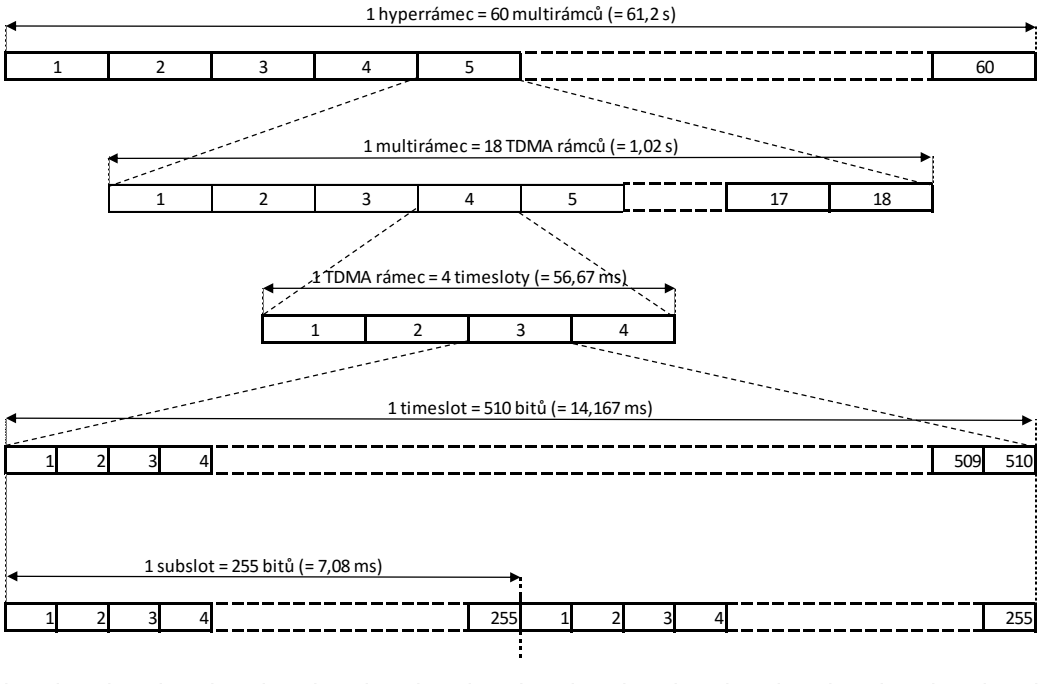
Rozhraní (č. 7) umožňuje propojení infrastruktury dodávané různými výrobci a umožňuje interoperabilitu mezi více sítěmi. Propojení pro přenos informací je možné pomocí komutovaného přenosu nebo paketového přenosu [17].

**Rozhraní pro síťový managment (Network Managment Interface)**

Umožňuje definovat požadavky pro správu sítě.

**Struktura rámců**

Rychlý přístup účastníka ke službám systému je stanoven metodou mnohonásobného přístupu MAP (Multiple Access Protocol). V systému TETRA byl zvolen mnohonásobný přístup s časovým dělením TDMA (Time Division Multiple Access) stejně jako v systému GSM. Oproti systému GSM obsahuje jeden TDMA rámec systému TETRA pouze 4 timesloty, které byly zvoleny jako kompromis nákladů na vytvoření infrastruktury a rozsah vyžadovaných služeb účastnických organizací.




Obrázek 4.4 Struktura TDMA systému TETRA

Obrázek 4.4 zobrazuje strukturu TDMA. V každém radiovém kanálu systému TETRA jsou metodou TDMA vytvořeny 4 časové intervaly, timesloty, které dohromady tvoří jeden TDMA rámec s periodou 56,67 ms [15]. Každý timeslot je tvořen 510 modulačními bity o délce trvání 14,167 ms. Pro uplink může být timeslot tvořen 2 subsloty o velikosti 255 bitů a trvání 7,08 ms. Spojením 18 TDMA rámců vzniká multirámec [15]. Poslední TDMA rámec označovaný také jako control frame, je použit výhradně pro řídící kanály. Dalším spojením 60 multirámců vzniká hyperrámec, který je nejvyšším stupněm hierarchie a má dobu trvání 61,2 s [15].

**Přenosové rychlosti**

Standard TEDS byl vyvinut k poskytnutí vyšší datové propustnosti. Umožňuje využívat celou řadu adaptivních modulačních schémat. Spolu s použitím různých šířek kanálu lze dosáhnout velkého rozsahu přenosových rychlostí, které jsou shrnuty v tabulce 4.1 [14]:

Tabulka 4.1 Přenosové rychlosti TEDS v závislosti na použité modulaci a šířce kanálu

| Modulace | Šířka kanálu (kHz) | | | |
|---|---|---|---|---|
| | 25 | 50 | 100 | 150 |
| π/4-DQPSK | 15,6 | | | |
| π/8-D8PSK | 24,3 | | | |
| 4-QAM (r=1/2) | 11 | 27 | 58 | 90 |
| 16-QAM (r=1/2) | 22 | 54 | 116 | 179 |
| 64-QAM (r=1/2) | 33 | 80 | 175 | 269 |
| 64-QAM (r=2/3) | 44 | 107 | 233 | 359 |
| 64-QAM (r=1) | 66 | 160 | 249 | 538 |

Přenosové rychlosti jsou uvedeny v kbit/s. Jedná se o maximální teoretické přenosové rychlosti, kdy se počítá s využitím všech 4 timeslotů. Uživatelská rychlost je vždy nižší než teoretická přenosová rychlost, která neuvažuje přenos dodatečných informací. Veličina *r*, značí rychlost kódování. Datová propustnost je lepší než u jiných technologií, ale přes velký pokrok v případě standardu TEDS, není stále dostatečná pro moderní multimediální aplikace. Někteří výrobci proto rozvíjí hybridní technologie s možností využitím 3G/LTE technologií.

### 4.3.2 Služby systému TETRA

Radiový systém TETRA umožňuje práci ve třech různých režimech [17]:

- Voice + data (V+D)
- Direct Mode Operation (DMO)
- Packet Data Optimised (PDO)

Nejpoužívanějším režimem je V+D, který umožňuje přepínání mezi řečí a přenosem dat. Při použití různých slotů v jednom kanále mohou být data i hlas přenášeny současně jednou stanicí. Režim podporuje plně duplexní provoz. Kromě standartních hovorových služeb umožňuje například skupinové volání, tísňové volání, naslouchání okolí a další.

Přímý operační režim DMO je druh provozu, kdy dvě nebo více mobilních stanic spolu komunikují bez použití spínací a řídící infrastruktury. Využívá se pro komunikaci v místech se slabým pokrytím signálu. Maximální dosah terminálů je v řádu jednotek kilometrů. Režim podporuje hlasové a datové služby, ale v tomto režimu není podporován plně duplexní spojení. Komunikace probíhá simplexně.

Režim PDO je optimalizován pouze pro přenos dat. V downlinku používá statistické časové multiplexování (STM). Od synchronního časového multiplexování se liší tím, že časové rámce se jednotlivým připojeným zařízením přiřazují dynamicky na základě momentálních potřeb, nikoliv po pevně daných opakujících se časových úsecích [12]. Nenastává tak případ, kdy je stanici přidělen časový rámec, přestože nemá co vysílat a tím je dosaženo lepší využití přenosové kapacity. Protože data příjemci nepřicházejí v periodicky se opakujících intervalech, musí být opatřena hlavičkou s identifikačními údaji. Tím vzniká dodatečná režie a hlavičky spotřebovávají část přenosové kapacity. V uplinku je použita metoda mnohonásobného přístupu STMA (STatistic Multiple Access).

**Skupinové volání**

Zahájení skupinového volání nastane v okamžiku, kdy první účastník vyšle požadavek systému. Systém na základě požadavku vyhradí systémové zdroje pro skupinové volání. Pokud jsou všechny kanály základnové stanice obsazeny, je požadavek zařazen do čekací fronty. Jakmile se kanály uvolní, jsou přiděleny pro čekající volání s nejvyšší prioritou. Systémové zdroje pro skupinová volání zůstávají vyhrazeny, dokud není systémem ukončeno pro překročení maximální délky hovoru, nebo při dostatečně dlouhé neaktivitě na komunikačním kanále. Dalším důvodem pro ukončení skupinového volání je uvolnění systémových zdrojů zatížené sítě pro uskutečnění nouzového volání [13].

Každá skupina má předem definováno území, na kterém může být aktivována. Toto území je definováno pokrytím buněk základnovými stanicemi. Stanice se může účastnit skupinového volání za předpokladu, že v daném okamžiku nachází na definovaném území a je členem skupiny. Pokud se účastník v rámci sítě pohybuje, o dostupnosti k jednotlivým skupinám je systémem informován na displeji stanice. Systém tak uživatele průběžně informuje, zda je v dosahu dané skupiny.

Během skupinového volání je na všech uživatelských a dispečerských stanicích účastníků zobrazena identifikace hovorové skupiny. Systémem je zároveň vysíláno upozornění o probíhajícím volání. Tím je umožněno připojení stanic, které před zahájením nebyly dostupné nebo do definovaného území vstoupily až po zahájení hovoru. Při skupinovém volání může v daném okamžiku hovořit pouze jedna stanice. Požadavek pro zahájení relace vysílá účastník stisknutím klíčovacího tlačítka. Pokud v daném okamžiku jiná stanice nehovoří, je požadavek přijat, v opačném případě je zařazen do fronty. Po skončení blokující relace je systémem z fronty vybrán požadavek s nejvyšší prioritou. Pokud uživatel uvolní klíčovací tlačítko, jeho žádost o relaci je z fronty vymazána.

**Tísňová volání**

Každý uživatel může vyvolat tísňové volání. Tísňový hovor dosahuje nejvyššího stupně priority. Důvodem je podmínka, že musí být uskutečněn za všech okolností. V případě vytíženosti sítě systém automaticky uvolní systémové zdroje obsazené relacemi s nejnižší prioritou. Systémové zdroje jsou tísňovému volání vyčleněny, dokud účastník nebo dispečer volání neukončí, nebo dokud neuplyne maximální délka hovoru. Volání je realizováno formou individuálního hovoru s dispečerem nebo skupinového hovoru. Hovor může být směřován na speciální tísňovou linku nebo na definovanou skupinu. Dispečer či účastnící skupiny jsou o aktivaci tísňového volání upozorněni.

Tísňová volání mohou být směřována do veřejné telefonní sítě nebo na pobočkovou ústřednu. Pobočková ústředna je schopna určit polohu volajícího. Na základě polohy je ústředna schopna hovor přesměrovat na číslo záchranné jednotky, která se nachází nejblíže místu uskutečnění hovoru. Účastník tak může v rámci celé sítě používat jedno předvolené číslo, přes které dojde k přesměrování hovoru do určené oblasti [13].

**Naslouchání okolí (Ambience Listening)**

Dispečer může převést radiostanici do režimu naslouchání bez jakékoliv indikace na terminálu účastníka. Tento režim umožňuje dispečerovi naslouchat zvukům v okolí radiostanice [17]. Tato funkce nachází specifické využití pro některé uživatelské aplikace, například v přepravě cenných a citlivých materiálů. Na druhou stranu, je tato služba zásahem do soukromí účastníka. Proto by měla být využívána pouze v aplikacích, které tuto funkci vyžadují.

**Dynamické skupiny**

Dynamic Group Number Assigment (DGNA) je služba, která umožňuje vytvářet a přidávat jedinečné skupiny uživatelů s odlišnými komunikačními potřebami. Nastavení mohou být aplikována pro účastníky již probíhajícího hovoru. Tato služba umožňuje členění uživatelů do definovaných skupin v rámci jedné organizace a zároveň nástroj pro usnadnění kooperace mezi více složkami, například policie, hasičů a zdravotní služby při řešení mimořádné události [17].

**Přidržení hovoru (Call Retention)**

Služba určuje vybrané uživatele, jejichž spojení nebude ukončeno během sestavení tísňového volání v přetížené sítí [17]. Z hlediska udržení funkcionality tísňového volání je důležité, aby počet těchto uživatelů byl co nejmenší.

**Autorizace hovoru dispečerem (Call Authorised by Dispatcher)**

Tato funkce umožňuje dispečerovi ověřit a schválit požadavky na hovor předtím, než hovor začne. Při žádosti o hovor dispečer obdrží jako údaj adresu volajícího, adresu volaného a základní požadavky na služby [17]. V případě, že nejsou splněny podmínky pro sestavení hovoru, je na volající stanici zasláno oznámení o zamítnutí hovoru.

**Pozdější vstup (Late Entry)**

Tato služba poskytuje možnost vstoupit do již probíhajícího hovoru účastníkům, kteří při sestavování hovoru nebyli k dispozici například z důvodu vypnutého terminálu, nacházeli se mimo pokrytí sítě nebo se účastnili jiného hovoru. Řídící kanál automaticky přesměruje terminál na základě výzvy hovorové skupiny, která již probíhá [17].

**Výběr oblasti (Area Selection)**

Touto funkcí správce sítě definuje pro jednotlivé oblasti parametry přenosu základnových radiostanic. Tato služba simuluje činnost dispečera pro výběr základnových stanic k uskutečnění hovoru. V sítí může být například zakázáno sestavit individuální hovor z důvodu uvolnění komunikačních zdrojů pro skupinová volání.

**Krátké datové přenosy**

Obdoba krátkých datových zpráv SMS systému GSM. Jedná se o datové přenosy o velikosti do 140 B, které se využívají pro krátké textové zprávy, sdílení informací o poloze protokolem LIP (Location Information Protocol) nebo pro stavové zprávy. Jednotlivé zprávy jsou od sebe odděleny pomocí identifikátoru zprávy. SDS zprávy lze posílat mezi účastníky, mezi účastníkem a dispečerem nebo účastník posílá zprávy do databáze systému. Pro poměrně krátkou délku trvání je datová zpráva přenášena přes řídící kanál TDMA rámce.

# 5 Praktická část

V praktické části jsem se zaměřil na použití spojovaného protokolu TCP (Tansmission Control Protcol), který patří mezi spojově orientované protokoly transportní vrstvy se spolehlivým doručováním. Předpoklad spolehlivého doručení dat považuji jako klíčové kritérium v případě komunikace během mimořádných událostí. Nespojově orientovaný protokol

Měření probíhalo v prostoru UTKO, konkrétně v místnosti SD5.69. Pro měření jsem měl k dispozici 2 notebooky a mobilní telefony Samsung Galaxy S4 obsahující sim karty amerického operátora AT&T (American Telephone and Telegraph). Oba smartphony byly přihlášeny k eNodeB1 sektoru 2 v kmitočtovém pásmu 700 MHz. Do notebooků bylo připojení k síti sdíleno jednotlivými smartphony za pomocí datového kabelu a zapnutí funkce USB tethering. Cílový server pro měření propustnosti se nacházel v EPC experimentální sítě za SeGW na ip adrese 172.30.32.101. Jednalo se o server pracující na linuxovém jádru Fedora.

## 5.1 Programové vybavení použité pro měření

### 5.1.1 Ping

Ping je základní softwarový nástroj pro testování dostupnosti síťového uzlu. Zároveň měří počet chyb, ztracených paketů a čas mezi vysláním zprávy ze zdrojového počítače a přijetím odpovědi od cílového počítače. Tento časový úsek označujeme jako latence. K provedení testu není zapotřebí žádný speciální software, ping je součástí všech operačních systémů, například příkazového řádku systémů Windows.

Základním parametrem pingu je doménové jméno nebo IP adresa síťového rozhraní, jehož dostupnost chceme prověřit. Pokud jako parametr uvedeme doménové jméno, je nejprve pomocí DNS (Domain Name Server) přeloženo na IP adresu. Ping využívá zprávy protokolu ICMP (Internet Control Message Protocol), konkrétně zprávu typu výzva, Echo Request, a zprávu typu odpověď – Echo reply.

Při zadání příkazu v základním tvaru v příkazovém řádku, tedy *ping cílová adresa*, uživatel jako výstup obdrží na výstupu zprávu obsahující ip adresu cílového počítače, velikost posílaných zpráv (standardně 32 bajtů) a 4 zprávy obsahující latenci pokusu, a celkové shrnutí obsahující minimální, maximální a průměrný čas odezvy. Kromě tohoto základního testu lze přídavnými příkazy ovlivnit parametry měření:

- **Ping -t** – Provádí testy do okamžiku, než je test přerušen uživatelem (v případě Windows klávesovou zkratkou CTRL+C).
- **Ping -n** – Provede *n* pokusů dostupnosti.
- **Ping -l** – Umožňuje nastavit velikost odesílané zprávy.

### 5.1.2 Iperf

Iperf je nástroj pro propustnosti a kvality spojení v síti. Program pracuje v serverovém a klientském režimu. Základem pro každé měření je spuštění serveru, na kterém chceme testovat propustnost sítě a jednoho klienta, který bude daný server testovat. Spuštěných aplikací v režimu serveru i klienta může být více, jednotlivé servery se od sebe budou lišit číslem portu, na kterém budou naslouchat. Nástroj iperf lze snadno nainstalovat na jakémkoliv operačním

systému UNIX/ Linux nebo Windows. Existují verze iperfu s grafickým rozhraním, ale v základním režimu lze iperf snadno spustit pomocí příkazové řádky.

Iperf v režimu server dokáže pracovat ve dvou režimech. Jedná se o režimy TCP a UDP. Rozdíly mezi těmito protokoly byly popsány v úvodu této kapitoly. V základním režimu bez použití parametrů příkazu běží server v módu TCP. Spuštění serveru v režimu UDP docílíme přidáním parametru -u. Při spuštění lze také nastavit číslo portu, na kterém bude server naslouchat.

Klientský režim iperfu spouštíme zadáním příkazu iperf s parametrem -c, za kterým následuje ip adresa testovaného serveru. Stejně jako u serveru je možné k příkazu přidat různé parametry. Parametry lze slučovat za sebe a docílit tak více specifického měření. Některé základní parametry jsou vypsány níže:

- **-u** – práce v režimu UDP
- **-p** – určení cílového portu
- **-t** – doba trvání testu v sekundách
- **-n** – množství dat, které má být odesláno v bajtech
- **-M** – velikost TCP segmentu
- **-i** – interval mezi vypsání přenosové rychlosti na výstup
- **-P** – simulace více paralelních testů
- **-d** -současný obousměrný test
- **-r** – postupný obousměrný test

Po zadání parametrů a proběhnutí testu dostane uživatel souhrn testu obsahující IP adresu a port testovaného serveru, velikost TCP segmentu, hodnoty přenesených dat a propustnost v daném intervalu. Názorný příklad výstupu:

```
------------------------------------------------------------
Client connecting to 172.30.32.101, TCP port 5001
TCP window size: 63.0 KByte (default)
------------------------------------------------------------
[  3] local 172.30.20.2 port 51011 connected with 172.30.32.101 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.2 sec  7.62 MBytes  6.26 Mbits/sec
```

## 5.2 Průběh měření

Pro testování propustnosti experimentální mobilní sítě jsem si stanovil 4 scénáře měření. Scénáře mají jednotnou strukturu měření. Před začátkem měření propustnosti sítě je v délce 10 sekund měřena odezva serveru, na kterém je spuštěn iperf v režimu server. V těchto měřeních dosahovala první odezva nepřiměřeně vysokých hodnot, řádově o desítky ms. Tento jev může být způsoben několika jevy. Jedním z důvodu je skutečnost, že MAC adresa cílového bodu není uložena v síťových prvcích, kterými prochází žádost o odezvu. Síťový prvek se tak prvně musí naučit cestu k určenému cílovému bodu. To způsobuje zpožděnou reakci na první ping. Navíc tyto záznamy ve směrovacích tabulkách jsou po krátké době vymazány, zde záleží na kontrétní

konfiguraci síťového prvku. Popsaná situace se tak opakuje na začátku každé měření. Z toho důvodu nejsou první odezvy zahrnuty do naměřených dat. Po testování odezvy nezatíženého serveru následuje samotné měření propustnosti programem iperf. Kontinuálně s měřením propustnosti opět probíhá měření latence serveru programem ping. Po skončení měření propustnosti následuje poslední série měření latence, trvající 10 sekund, měřící odezvu serveru po skončení zátěže.

Jednotlivé scénáře jsou dále provedeny ve 4 variantách. Rozdíly mezi jednotlivými variantami spočívají v délce průběhu testu měření propustnosti sítě. Varianta A (označovaná jako VA) spočívá v měření propustnosti v délce trvání 10 sekund. Parametrem -i na straně klienta byl nastaven periodický výpis naměřené posloupnosti v intervalu jedné vteřiny. Při variantě B (VB) je propustnost měřena po dobu 30 sekund s periodou výpisu propustnosti 5 sekund. Následují 2 krátkodobé scénáře, varianta C (VC) s dobou měření 5 vteřin ve vteřinových intervalech a varianta D (VD) s dobou měření propustnosti v délce 2 sekund. Pro scénáře B,C a D, které zahrnují připojení 2 zařízení byly vytvořeny scénáře i pro zařízení, jehož úkolem je ovlivnit kritické zařízení. V případě druhého zařízení nebyly měřeny hodnoty propustnosti ani latence.

Jednotlivé scénáře jsem nakonfiguroval do 2 dávkových souborů s připonou *.bat*. Důvodem pro vytvoření bylo automatizace měření místo jednotlivých zadávání příkazů a docílení synchronizace měření propustnosti sítě programem iperf a odezvy serveru programem ping. Za normálních okolností při sekvenci příkazů probíhají jednotlivé příkazy za sebou, vždy po skončení předchozího. Prvním dávkovým souborem je soubor *test.bat*. Jako první příkaz obsahuje příkaz ping pro měření latence před započtením testu propustnosti. Výstup prvního testu latence jsem přesměroval do textového souboru *ping1.txt*. Pro simultánní měření propustnosti a odezvy jsem opatřil druhý příkaz parametrem start, který vytvoří novou instanci programu, kontrétně spustí soubor *propustnost.bat* obsahující příkaz spuštění iperf clienta a měření propustnosti serveru. Výpis tohoto měření je přesměrován do souboru *propustnost.txt*. Zároveň se souborem *propustnost.bat* pokračuje posloupnost příkazů v prvním dávkovacím souboru. Dalšími příkazy jsou 2 testy odezvy, první během měření posloupnosti, druhý po ukončení měření propustnosti. Výstupy obou testů jsou opět přesměrovány do textových sobourů *ping2* a *ping3*.

Ilustrační příklad souboru *test.bat*:

```
ping 172.30.32.101 -n 10 >> d:\VUT\TCP\S1\D\ping1.txt
start d:\VUT\TCP\S1\D\propustnost.bat
ping 172.30.32.101 -n 2 >> d:\VUT\TCP\S1\D\ping2.txt
ping 172.30.32.101 -n 10 >> d:\VUT\TCP\S1\D\ping3.txt
```

následuje příklad zápisu v souboru *propustnost.bat*:

```
d:\VUT\iperf -c 172.30.32.101 -p 5001 -i 1 -t 2 >> d:\VUT\TCP\S1\D\propustnost.txt
exit
```

### 5.2.1 Scénář 1

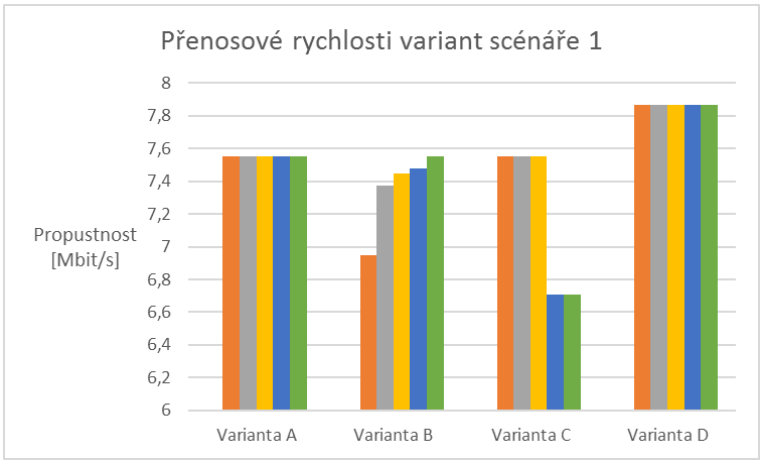
Tento základní scénář simuluje připojení zařízení do mobilní sítě. Jelikož síť není zatížena jiným provozem, předpokladem pro toto měření je dosáhnutí nejvyšší propustnosti sítě a nejnižší latence. Průměrné hodnoty propustnosti jsou shrnuty v tabulce 5.1 a poté vyneseny do grafu na obrázku 5.1, průměrné délky odezvy pak v tabulce 5.2 a na obrázku 5.2. Průměrná propustnost sítě se pohybovala kolem hodnoty 7,5 Mbit/s s dobou odezvy 65 ms. Tyto hodnoty budou výchozí pro porovnání s hodnotami zbylých scénářů, protože při tomto měření neobsluhoval server žádné jiné zařízení.

Tabulka 5.1 Průměrné hodnoty propustnosti sítě scénáře 1

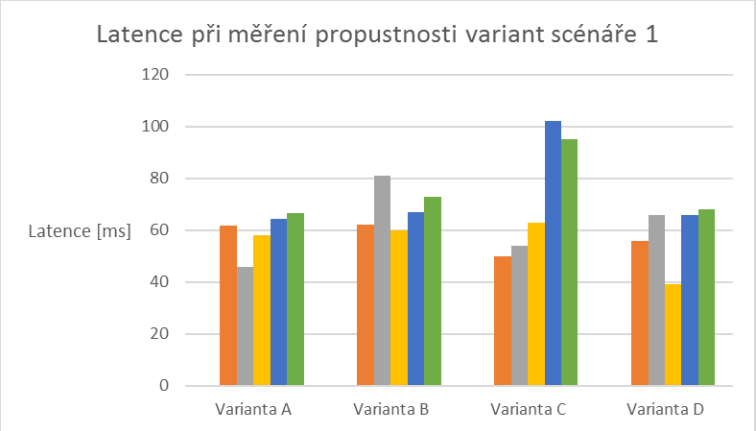
| Propustnost [Mbit/s] | Měření 1 | Měření 2 | Měření 3 | Měření 4 | Měření 5 |
|---|---|---|---|---|---|
| Varianta A | 7,55 | 7,55 | 7,55 | 7,55 | 7,549 |
| Varianta B | 6,95 | 7,375 | 7,445 | 7,48 | 7,55 |
| Varianta C | 7,55 | 7,55 | 7,55 | 6,71 | 6,71 |
| Varianta D | 7,865 | 7,865 | 7,865 | 7,865 | 7,865 |

Tabulka 5.2 Průměrná délka odezvy při měření propustnosti scénáře 1

| Latence při měření propustnosti [ms] | Měření 1 | Měření 2 | Měření 3 | Měření 4 | Měření 5 |
|---|---|---|---|---|---|
| Varianta A | 61,6 | 45,9 | 57,9 | 64,4 | 66,7 |
| Varianta B | 62 | 81 | 60 | 67 | 73 |
| Varianta C | 50 | 54 | 63 | 102 | 95 |
| Varianta D | 56 | 66 | 39 | 66 | 68 |




Obrázek 5.1 Graf průměrných propustností sítě při měření variant scénáře 1




Obrázek 5.2 Graf průměrných hodnot latencí při měření propustnosti podle scénáře 1

### 5.2.2 Scénář 2

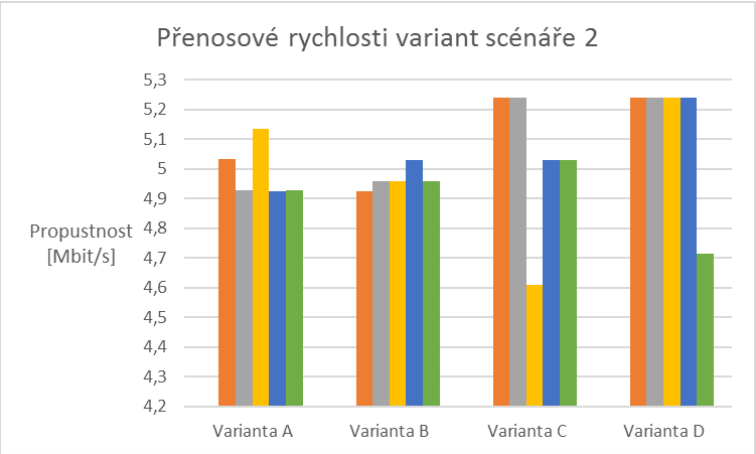
Stejně jako ve scénáři 1 je výchozím stavem nezatížená síť. Tento scénář simuluje situaci, kdy se ve stejné síti nachází zařízení, které periodicky od nadřazené aplikace obdrží data, například výzvu k provedení definované činnosti. Při aplikování stejného intervalu pro obě zařízení dochází k situaci, kdy obě zařízení vyžadují od serveru data ve stejný okamžik. Kapacita sítě se tak dělí mezi obě zařízení. Podle očekávání byly naměřeny nižší hodnoty propustnosti v průměru 5 Mbit/s, které zobrazuje tabulka 5.3 a obrázek 5.3. Naopak doba odezvy se zvýšila průměrně na hodnotu 90 ms, viz tabulka 5.4 a obrázek 5.4.

Tabulka 5.3 Průměrné hodnoty propustnosti sítě scénáře 2

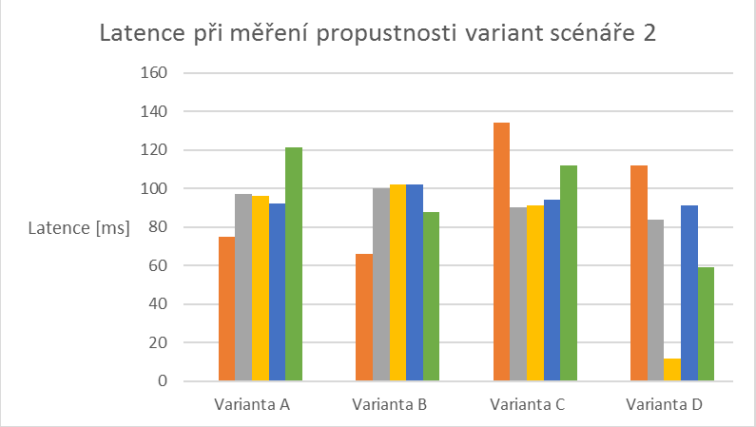
| Propustnost [Mbit/s] | Měření 1 | Měření 2 | Měření 3 | Měření 4 | Měření 5 |
|---|---|---|---|---|---|
| Varianta A | 5,032 | 4,928 | 5,136 | 4,926 | 4,928 |
| Varianta B | 4,925 | 4,96 | 4,96 | 5,03 | 4,96 |
| Varianta C | 5,24 | 5,24 | 4,61 | 5,03 | 5,03 |
| Varianta D | 5,24 | 5,24 | 5,24 | 5,24 | 4,715 |

Tabulka 5.4 Průměrná délka odezvy při měření propustnosti scénáře 2

| Latence při měření propustnosti [ms] | Měření 1 | Měření 2 | Měření 3 | Měření 4 | Měření 5 |
|---|---|---|---|---|---|
| Varianta A | 75 | 97 | 96,1 | 92,2 | 121,5 |
| Varianta B | 66 | 100 | 102 | 102 | 88 |
| Varianta C | 134 | 90 | 91 | 94 | 112 |
| Varianta D | 112 | 84 | 12 | 91 | 59 |




Obrázek 5.3 Graf průměrných propustností sítě při měření variant scénáře 2




Obrázek 5.4 Graf průměrných hodnot latencí při měření propustnosti podle scénáře 2

### 5.2.3 Scénář 3

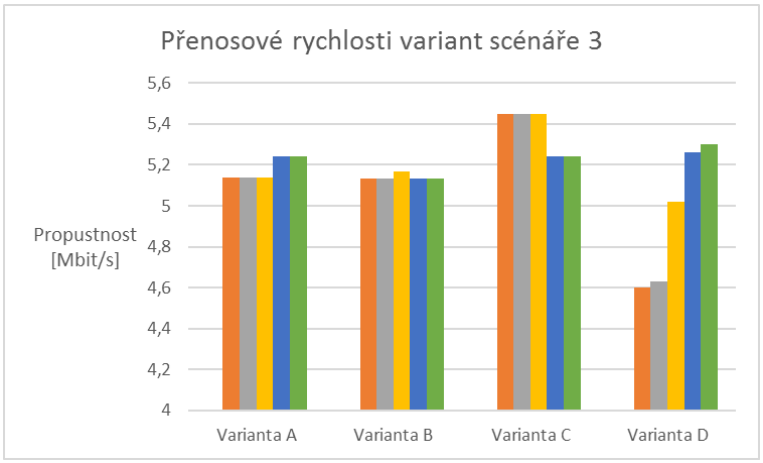
Výchozím stavem pro měření je stálý provoz na pozadí sítě. Tento scénář simuluje situaci, kdy se do zatížené sítě připojí kritické zařízení. Testované zařízení je připojeno do sítě a je mu přidělena přenosová kapacita závislá na míře zatížení sítě. V případě scénáře 3 dosahovala přenosová rychlost průměrně hodnoty 5,2 Mbit/s viz tabulka 5.5, obrázek 5.5. Mírně vyšších hodnot dosahovaly scénáře C a D, které simulovaly připojení zařízení na 5 sekund a 2 sekundy. Tyto scénáře zároveň vykazovaly nižší dobu odezvy, řádově 30 až 40 ms oproti variantě měření A a B. Průměrná doba odezvy 81 ms, je tak v tomto případě zavádějící. Data z měření odezvy jsou zobrazeny v tabulce 5.6 a na obrázku 5.6.

Tabulka 5.5 Průměrné hodnoty propustnosti sítě scénáře 3

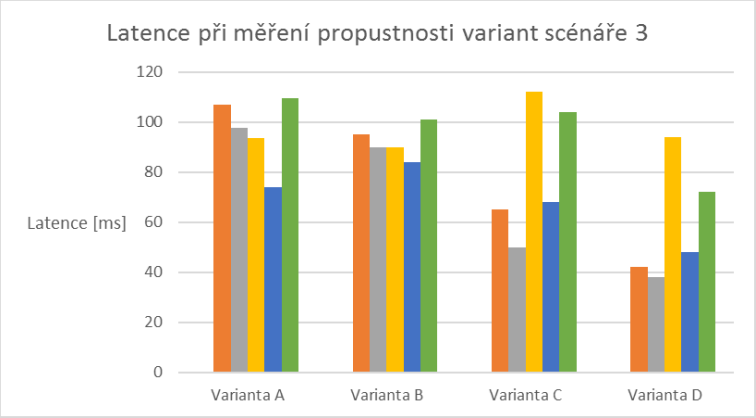
| Propustnost [Mbit/s] | Měření 1 | Měření 2 | Měření 3 | Měření 4 | Měření 5 |
|---|---|---|---|---|---|
| Varianta A | 5,136 | 5,138 | 5,136 | 5,242 | 5,242 |
| Varianta B | 5,135 | 5,135 | 5,17 | 5,135 | 5,135 |
| Varianta C | 5,45 | 5,45 | 5,45 | 5,24 | 5,24 |
| Varianta D | 4,6 | 4,63 | 5,02 | 5,26 | 5,3 |

Tabulka 5.6 Průměrná délka odezvy při měření propustnosti scénáře 3

| Latence při měření propustnosti [ms] | Měření 1 | Měření 2 | Měření 3 | Měření 4 | Měření 5 |
|---|---|---|---|---|---|
| Varianta A | 106,7 | 97,8 | 93,5 | 74 | 109,5 |
| Varianta B | 95 | 90 | 90 | 84 | 101 |
| Varianta C | 65 | 50 | 112 | 68 | 104 |
| Varianta D | 42 | 38 | 94 | 48 | 72 |




Obrázek 5.5 Graf průměrných propustností sítě při měření variant scénáře 3




Obrázek 5.6 Graf průměrných hodnot latencí při měření propustnosti podle scénáře 3

### 5.2.4 Scénář 4

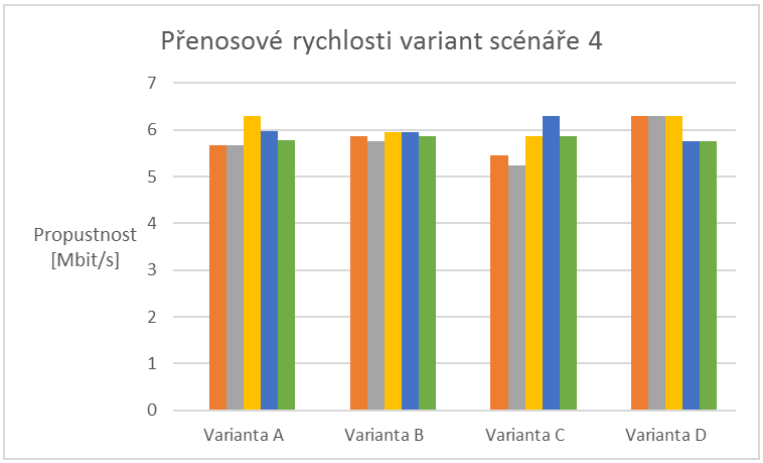
V tomto scénáři probíhá na pozadí provoz v krátkých časových úsecích, tzv. burstech. Testované zařízení je připojeno do sítě a po zadaný interval je testována jeho propustnost. Během měření několikrát dochází k přerušení a opětovnému navázání spojení na pozadí. Tyto změny v zatížení sítě se projevují v průběžných změnách dosažené přenosové kapacity testovaného zařízení. Propustnost dosahovala hodnot 5,6 až 6,2 Mbit/s, v rámci měření v jednotlivých variantách se rozdíly pohybovaly až do velikosti 0,5 Mbit/s, což je jednoznačně největší kolísavost. V ostatních scénářích k tak velké kolísavosti docházelo pouze ojediněle.

Tabulka 5.7 Průměrné hodnoty propustnosti sítě scénáře 4

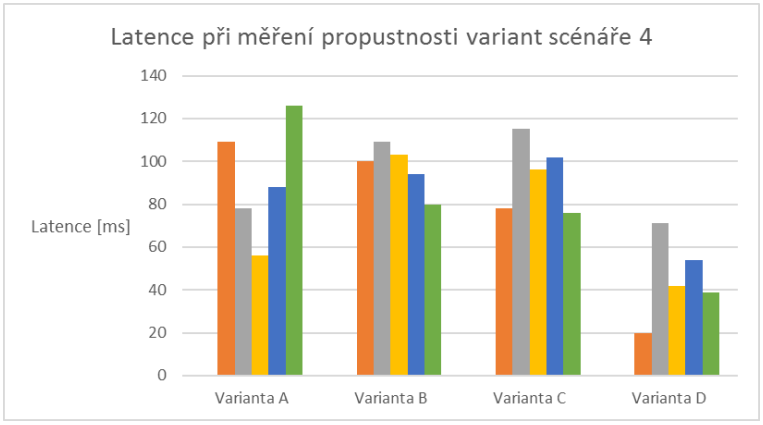
| Propustnost [Mbit/s] | Měření 1 | Měření 2 | Měření 3 | Měření 4 | Měření 5 |
|---|---|---|---|---|---|
| Varianta A | 5,662 | 5,66 | 6,294 | 5,978 | 5,768 |
| Varianta B | 5,87 | 5,765 | 5,94 | 5,94 | 5,87 |
| Varianta C | 5,45 | 5,24 | 5,87 | 6,29 | 5,87 |
| Varianta D | 6,29 | 6,29 | 6,29 | 5,765 | 5,765 |

Tabulka 5.8 Průměrná délka odezvy při měření propustnosti scénáře 4

| Latence při měření propustnosti [ms] | Měření 1 | Měření 2 | Měření 3 | Měření 4 | Měření 5 |
|---|---|---|---|---|---|
| Varianta A | 109 | 78 | 56 | 88 | 126 |
| Varianta B | 100 | 109 | 103 | 94 | 80 |
| Varianta C | 78 | 115 | 96 | 102 | 76 |
| Varianta D | 20 | 71 | 42 | 54 | 39 |




Obrázek 5.7 Graf průměrných propustností sítě při měření variant scénáře 4




Obrázek 5.8 Graf průměrných hodnot latencí při měření propustnosti podle scénáře 4

## 5.3 Závěr měření

Cílem tohoto měření bylo analyzovat možnosti podpory komunikace kritických koncových zařízení. Pro toto měření byly vytvořeny 4 scénáře, každý ve 4 variantách, které představovaly některé možné situace síťového provozu. Při použití omezeného počtu připojených zařízení do sítě nemohlo být dosaženo situace, aby kritické zařízení nebylo sítí obslouženo. Proto se toto měření zaměřilo na změny propustnosti sítě v závislosti na jednotlivých scénářích. Jako výchozí stav byl použit scénář, kdy se kritické zařízení připojuje do sítě bez dalšího provozu. Největší změny v průběhu propustnosti byly analyzovány ve scénáři 4, kdy do komunikace neustále zasahovaly datové toky s malou velikostí ale velkou frekvencí. Tento fakt dokládá potřebu klást důraz na prioritizaci v rámci síťové infrastruktury mobilní sítě.

# Závěr

Cílem této bakalářské práce bylo popsat možnosti využití komerčních mobilních sítí na podporu kritické infrastruktury.

V první kapitole jsem se věnoval vysvětlení základních pojmů problematiky kritické infrastruktury a uvedl jsem rozdělení prvků kritické infrastruktury podle odvětvových kritérií do jednotlivých oblastí a služeb.

Ve druhé kapitole jsem popsal technologie, které docílí zvýšené integraci prvků jednotlivých oblastí kritické infrastruktury a komunikačními a informačními technologiemi. Tyto technologie budou implementovány do standardu mobilních sítí a umožní tak zvýšit zabezpečení kritické infrastruktury státu.

Ve třetí části jsem po technické stránce popsal možnost použití komerčních mobilních sítí pro podporu kritické infrastruktury. Tyto možnosti na základě technologií popsané ve druhé kapitole popisuje standard LTE D2D. Dále jsem nastínil konkrétní možnosti využití v oblastech energetiky, zdravotnictví, průmyslu a služeb.

Čtvrtá kapitola se věnovala požadavkům na mobilní sítě v případě mimořádné události. V úvodní jsem popsal strukturu integrovaného záchranného systému a uvedl současné uplatnění komerčních mobilních sítí ve zprostředkování přístupu k tísňové lince. V další části jsem se věnoval radiové svazkové síti TETRA, která byla vyvinuta právě z důvodu použití v kritické infrastruktuře a při mimořádných událostech. Analyzoval jsem klíčové charakteristiky systému a uvedl specifické funkce, kterými se TETRA vyznačuje. Jedná se především o možnost vytvoření skupinových volání, vytváření dynamických skupin a možnost přidělovat jednotlivým účastníkům různě stupně priority komunikace. Nevýhodou systému TETRA tkví především v malých datových přenosech, které již nedostačují dnešním potřebám, například pro multimediální přenosy.

V poslední kapitole jsem popsal měření komunikace realizované v experimentální mobilní sítí UTKO. Před samotným měřením jsem si vytvořil 4 scénáře pro měření. Jednotlivé scénáře představovaly specifické situace, které mohou během datových přenosů nastat. Každý ze scénářů se dále skládal ze 4 variant, které se od sebe lišily délkou měření propustnosti sítě. Na základě naměřených dat jsem analyzoval míru ovlivnění měřených veličin jednotlivými scénáři.

# Seznam použité Literatury


[1] Accelerating IoT. *Ericsson* [online]. 2015, 10. 9. 2015 [cit. 2015-12-10]. Dostupné z: http:/www.ericsson.com/news/150910-accelerating-iot_244069645_c

[2] HRSTKA, Jaroslav. Kudy vede cesta k úspěchu M2M. *Sdělovací technika*. Praha: Sdělovací technika, 2014, 61(6): 3. ISSN 0036-9942.

[3] The many faces of IoT (Internet of Things) in Healthcare. *Slideshare* [online]. 2014, 12. 11. 2014 [cit. 2015-12-10]. Dostupné z: http://www.slideshare.net/stockerpartnership/the-many-faces-of-internet-of-things-iot-in-healthcare

[4] Private LTE for Critical Infrastructure [online]. In: Motorola, ENTELEC, 2013. Dostupné z: https://higherlogicdownload.s3.amazonaws.com/ENTELECCOMMUNITY/44abb782-c5b7-4380-8cad-18966390f503/UploadedImages/

[5] Telekomunikační věstník: Číslovací plán veřejných telefonních sítí. *Český telekomunikační úřad* [online]. [cit. 2015-12-13]. Dostupné z: https://www.ctu.cz/cs/download/cislovaci-plany-archiv/cislovaci-plan-verejnych-telefonnich-siti-1114435245.pdf

[6] STEIN, Willi. *Criticial infrastructure protection: Status and perspecvites* [online]. Frankfurt, 2003 [cit. 2015-12-13]. Dostupné z: http://www1.gi-ev.de/fachbereiche/sicherheit/fg/kritis/CIP-Workshop-GI-03.pdf

[7] ČAREK, Jan. Internet of Things: Plíživý nástup technologické revoluce. *Cnews.cz* [online]. 2. 4. 2015 [cit. 2015-12-15]. Dostupné z: http://www.cnews.cz/clanky/internet-things-plizivy-nastup-technologicke-revoluce

[8] VÍTEK, Jan. Internet of Things: Propojená budoucnost. *Svět hardware: vše ze světa počítačů* [online]. 2014, 9. 12. 2015 [cit. 2015-12-15]. Dostupné z: http://www.svethardware.cz/internet-of-things-propojena-budoucnost/39560

[9] Cloud computing. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-12-15]. Dostupné z: https://en.wikipedia.org/wiki/Cloud_computing

[10] Machine to Machine (M2M) Communications: Part 1: Basics and Challenges. *Ericsson* [online]. [cit. 2015-12-15]. Dostupné z: https://www.kth.se/social/upload/51361070f27654791e77d70d/MachineToMachineCommunicationsPartI.pdf

[11] ČESKÁ REPUBLIKA. Zákon o krizovém řízení a o změně některých zákonu: Krizový zákon. In: 2000. 240/2000 Sb. Dostupné také z: https:/portal.gov.cz/app/zakony/download?idBiblio=49557

[12] PETERKA, Jiří. Přenosové techniky: Multiplexování. In: *Archiv článků Jiřího Peterky* [online]. [cit. 2016-05-20]. Dostupné z: http://www.earchiv.cz/a96/a651k150.php3

[13] Digitální rádiové sítě TETRA. In: Echoton [online]. [cit. 2016-05-19]. Dostupné z: http://www.echoton.cz/mobilni-komunikace/digitalni-radiove-site-tetra.html

[14] POOLE, Ian. TETRA: Terrestrial Trunked Radio System. In: *Radio-Electronics* [online]. [cit. 2016-05-21]. Dostupné z:

http://www.radio-electronics.com/info/pmr-business-land-mobile-radio/tetra/what-is-tetra-radios-communications.php
[15] EUROPEAN TELECOMMUNICATION STANDARD. *Terrestrial Trunked Radio (TETRA): Voice plus Data (V+D)* [online]. 1999, 780 s. [cit. 2016-05-21]. ETS 300 392-2. Dostupné z: http://www.etsi.org/deliver/etsi_i_ets/300300_300399/30039202/02_20_200015/ets_30039202e02c.pdf
[16] Terrestrial Trunked Radio. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-05-21]. Dostupné z: https://cs.wikipedia.org/wiki/Terrestrial_Trunked_Radio
[17] TETRA. *TCCA: TETRA - Critical Communications Association* [online]. [cit. 2016-05-22]. Dostupné z: http://www.tandcca.com/about/page/12030
[18] BRYDON, Alastair. Opportunities and threats from LTE Device-to-Device (D2D) communication. In: Unwired Insight [online]. 2014 [cit. 2016-05-25]. Dostupné z: http://www.unwiredinsight.com/2014/lte-d2d
[19] SCHLIENZ a ROESSLER. Device to Device Communication in LTE. In: Rohde & Schwarz [online]. [cit. 2016-05-25]. Dostupné z: http://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma264/1MA264_0e_D2DComm.pdf
[20] POOLE, Ian. 4G LTE Device to Device, D2D. In: Radio-Electronics [online]. [cit. 2016-05-26]. Dostupné z: http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/4g-lte-advanced-d2d-device-to-device.php

# Seznam zkratek

| | |
|---|---|
| 3GPP | The third Generation Partnership Project |
| ABS | Anti-lock Brake System |
| AT&T | American Telephone and Telegraph |
| ČR | Česká republika |
| D2D | Device to Device |
| DGNA | Dynamic Group Number Assigment |
| DMO | Direct Mode Operation |
| DNS | Domain Name Server |
| EMC | Elektromagnetická kompatibilita |
| EPC | Evolved Packet Core |
| ETSI | European Telecommunications Standards Institute |
| EU | Evropská Unie |
| E-UTRAN | Evolved UMTS Terrestrial Radio Access |
| FDMA | Frequency Disivion Multiple Access |
| H2H | Human to Human |
| IaaS | Infrastructure as a Service |
| ICMP | Internet Control Message Protocol |
| IoT | Internet of Things |

| | |
|---|---|
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| IZS | Integrovaný záchranný systém |
| KI | Kritická infrastruktura |
| LIP | Location Information Protocol |
| LTE | Long Term Evolution |
| M2H | Machine to Human |
| M2M | Machine to Machine |
| MAP | Multiple Access Protocl |
| MCC | Mobile Country Code |
| MMI | Man-Machine Interface |
| MNC | Mobile Network Code |
| MS | Mobile Station |
| NMS | Network Managment Systém |
| PaaS | Platform as a Service |
| PDO | Packet Data Optimised |
| PEI | Peripheral Equipment Interface |
| Ping | Packet InterNet Gropper |
| PTT | Push To Talk |
| RBS | Radio Base Station |
| RFID | Radio Frequency Identification |
| RLS | Remote Line Station |
| SaaS | Software as a Service |
| SCN | Switching Controller Node |
| SwMI | Switching and Management Infrastructure |
| TCP | Transmission Control Protocol |
| TDMA | Time Division Multiple Access |
| TEDS | TETRA Enhanced Data Service |
| TETRA | TErrestrial Trunked RAdio |
| TMO | Trunked Mode Operation |
| UDP | User Datagram Protocol |
| UE | User Equipment |
| V+D | Voice + Data |
| WiFi | Wireless Fidelity |