VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ
INSTITUTE OF FORENSIC ENGINEERING

ODBOR INŽENÝRSTVÍ RIZIK
DEPARTMENT OF RISK ENGINEERING

MOBILNÍ SÍTĚ JAKO KRITICKÁ INFRASTRUKTURA A JEJICH RIZIKA

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Ing. Radko Krkoš, Ph.D.

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Jana Victoria Martincová, Ph.D.

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

Zadání diplomové práce

Student:	**Ing. Radko Krkoš, Ph.D.**
Studijní program:	Řízení rizik technických a ekonomických systémů
Studijní obor:	Řízení rizik technických systémů
Vedoucí práce:	**Ing. Jana Victoria Martincová, Ph.D.**
Akademický rok:	2020/21
Ústav:	Odbor inženýrství rizik

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Mobilní sítě jako kritická infrastruktura a jejich rizika

Stručná charakteristika problematiky úkolu:

Popište možnosti využití mobilních buňkových sítí ve funkci zabezpečení komunikačních strategických potřeb státu i komerčních subjektů.
Realizujte analýzu rizik, ve kterých jsou mobilní sítě nebo jejich části chráněnými aktivy a sekundárně také zdroji rizik. Zaměřte se na realizaci funkcí kritické infrastruktury za běžného provozu ale zejména v případě mimořádných událostí nebo stavu nebezpečí. Diskutujte technická a organizační opatření pro ochranu funkcí kritické infrastruktury v mobilních sítích.

Cíle diplomové práce:

Posouzení rizik mobilní sítě jako kritické infrastruktury.

Seznam doporučené literatury:

[1] Zákon č. 240/2000 Sb.: Zákon o krizovém řízení a o změně některých zákonů (krizový zákon). Česká republika, 2000, ročník 2000, číslo 240.

[2] Mission Critical Services in 3GPP. 3GPP: 3rd Generation Partnership Project [online]. 2017 [cit. 2019-04-14]. Dostupné z:

https://www.3gpp.org/news-events/3gpp-news/1875-mc_services

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně, dne

L. S.

Ing. Jana Victoria Martincová, Ph.D. vedoucí odboru	prof. Ing. Karel Pospíšil, Ph.D., LL.M. ředitel

ABSTRAKT

Práce se zaobírá problematikou mobilních buňkových sítí, fungujících v roli kritické infrastruktury, na základě systémového přístupu, obecných metod analýzy rizik a specializovaných metod pro diagnostiku a analýzu vycházejících z inženýrské praxe v oblasti provozu mobilních buňkových sítí.

KLÍČOVÁ SLOVA

mobilní buňková síť, analýza rizik, systémový přístup, diagnostika

ABSTRAKT

Práca sa zaoberá problematikou mobilných bunkových sietí, fungujúcich v roli kritickej infraštruktúry, na základe systémového prístupu, obecných metód analýzy rizík a špecializovaných metód pre diagnostiku a analýzu vychádzajúcich z inžinierskej praxe v oblasti prevádzky mobilných bunkových sietí.

KĽÚČOVÉ SLOVÁ

mobilná bunková sieť, analýza rizík, systémový prístup, diagnostika

ABSTRACT

This document deals with the topic of mobile cellular networks, operating as a critical infrastructure, based on systemic approach, general risk analysis methods and specialized methods for diagnostics and analysis founded on technical praxis from running mobile cellular networks.

KEYWORDS

mobile cellular network, risk analysis, systemic approach, diagnostics

KRKOŠ, Radko. *Mobilní sítě jako kritická infrastruktura a jejich rizika*. Brno, 2021. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/120410. Diplomová práce. Vysoké učení technické v Brně, Ústav soudního inženýrství, Odbor inženýrství rizik. Vedoucí práce Jana Victoria Martincová.

Prehlásenie

Prehlasujem, že svoju diplomovú prácu na tému „*Mobilní sítě jako kritická infrastruktura a jejich rizika*“ som vypracoval samostatne s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce. Ako autor uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných alebo majetkových a som si plne vedomý následkov porušenia ustanovení § 11 a nasledujúcich autorského zákona č. 121/2000 Sb. ČR, o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovení časti druhej, hlavy VI. dielu 4 Trestného zákonníku č. 40/2009 Sb. ČR.

V Brne ....

(podpis autora)

Poďakovanie

Ako autor tejto záverečnej práce by som sa chcel poďakovať pôvodnému vedúcemu práce prof. Ing. Vladimírovi Adamcovi, CSc. za metodickú a odbornú gesciu pri jej vypracovávaní, ďalej za poskytnuté rady a usmernenia.

Ďalej by som chcel poďakovať pani Jane Makovičkovej, pracovníčke študijného oddelenia ÚSI VUT, za pomoc pri riešení nútenej zmeny vedúceho práce kvôli personálnym zmenám na ústave.

Tiež by som chcel poďakovať náhradnej vedúce práce, pani Ing. Jane Victorii Martincovej, Ph.D., za možnosť pokračovať v práci a v neposlednom rade tiež za metodickú pomoc a poskytnuté rady a usmernenia.

V Brne ....

(podpis autora)

Obsah

Úvod

Kritická infraštruktúra z pohľadu nejakého systému je taká infraštruktúra, ktorá poskytuje súbor nutných podporných služieb pre realizáciu základných a doplnkových funkcií tohto systému. Ľudská spoločnosť je založená na komunikácií jej členov, čiže predávaní informácií medzi nimi. Akákoľvek organizačná štruktúra tvorí ďalšie štruktúry a systémy tak, že kopírujú organizáciu tej čo ich vytvorila. Technické systémy vytvorené ľuďmi sú tiež založené na vzájomnej komunikácií, teda výmene dát.

Mobilné komunikačné siete sú dnes všeobecne dostupné, dokonca aj v rozvojových krajinách, a stali sa majoritným komunikačným prostriedkom pre väčšinu populácie, mnohé priemyselné odvetvia a služby. Mobilná komunikácia je pre používateľov pohodlná a vytvára situáciu, keď prakticky každý má neustále so sebou výkonný výpočtový nástroj s pripojením ku globálnej komunikačnej sieti a teda prístup k zbierke vedomostí ľudstva. Z nástroja zvýšenia komfortu komunikácie a osobného asistenta sa teda stala kritická infraštruktúra, pretože pre mnohých používateľov, ľudských či technických, sa v niektorých situáciách jedná o jediný spôsob zabezpečenia potreby komunikácie.

Táto práca sa zaoberá prevádzkou mobilných bunkových sietí v rolách kritickej infraštruktúry, ako z pohľadu štátu a spoločnosti, tak iných kritických infraštruktúr, technických systémov či ľudí ako jednotlivcov. Sú skúmané riziká ohrozujúce súčasti mobilných sietí a tiež výsledného komunikačného systému ako celku. Ďalej sa prihliada na to, že akákoľvek kritická infraštruktúra musí byť bezpečná pre svoje okolie a používateľov, aby mohla plniť svoj účel. Preto sú skúmané tiež riziká, kde je mobilná sieť zdrojom ohrozenia.

Pre porozumenie akémukoľvek zariadeniu, deju, javu či procesu je nutné poznať ich štruktúru, vzťahy medzi súčasťami a vzťahy a možné interakcie s okolím. Pre komplexné systémy je táto potreba výraznejšia, pretože množstvo možných vnútorných aj vonkajších interakcií a teda požadovaného poznania stúpa multiplikatívne. Systémy je teda nutné modelovať na vhodnej úrovni detailnosti pre nadväzujúcu analýzu možných zraniteľností a hrozieb. S touto úlohou pomáha systémový prístup, ktorý je pri realizácii tejto práce použitý.

Obecne inžinierska prax vyžaduje aplikáciu dostupných znalostí pre riešenie problémov a zlepšovanie stavu, spoľahlivosti a možností technických zariadení. Akékoľvek skúmanie technických systémov teda nemôže zostať len v teoretickej rovine, ale je nutné overiť aj súvis vyskúmaného s realitou. V rámci tejto práce sa preto navrhnuté a diskutované postupy tiež overujú v existujúcich, komerčne prevádzkovaných, inštaláciách.

V neposlednom rade je mobilná sieť fascinujúcim technickým dielom, založenom na systémovej a intenzívnej špičkovej odbornej práci mnohých ľudí - vedcov, inžinierov a technikov. Táto práca by mala čitateľa uviesť do uvedenej časti ľudskej činnosti – problematiky mobilných bunkových sietí.

1 Literárna rešerš problematiky

Predkladaný text v mnohých oblastiach nie je výsledkom originálneho výskumu a preto boli pri jeho vyhotovení používané odborné zdroje. V tejto kapitole sú zdroje použité v práci stručne charakterizované. Viaceré zdroje spolu súvisia a celkovo ich je možné rozdeliť do niekoľkých tematických oblastí.

Prvým tematickým celkom sú zákony ako dokumenty upravujúce práva a povinnosti orgánov štátnej a verejnej správy, či fyzických a právnických osôb. Základným legislatívnym dokumentom, z ktorého v právnom štáte vychádza legislatíva ostatná, je ústava. Ústava ČR (Česká republika) [1] a vzhľadom na kultúrnu blízkosť aj Ústava SR (Slovenská republika) [2] definujú rámec úpravy práv a povinností. t.j. aké povinnosti je vôbec možné občanom ukladať, preto právna analýza začína vždy tam. Na ústavu nadväzuje z pohľadu správy kritickej infraštruktúry Zákon o krízovom riadení č. 240/2012 Sb. [4], ktorý do národnej legislatívy implementuje obsah Smernice EU (Európska únia) č. 2008/114 [3] o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. Problematiku ochrany komunikačných systémov pred kybernetickými hrozbami rieši zákon č. 181/2014 Sb. [5]. Smernice EU sú publikované okrem úradného vestníku EU tiež na webovej stránke https://eur-lex.europa.eu/ vo všetkých úradných jazykov členských krajín EU, pretože musia byť dostupné občanom, odkaz na [3] je teda doplnený aj URL[1] dokumentu na tejto webovej službe. Primárnym zdrojom pre národnú legislatívu je zbierka zákonov, pravidelne publikovaná vydávajúcou krajinou. Práca s legislatívou v tejto forme je ale náročná, najmä pre množstvo aktualizácii a vzájomných vplyvov zákonov, vyhlášok a nariadení. Pre praktické použitie je dôležité získať konkrétny zákon v aktuálnom znení, prípadne v špecifických situáciách v znení ku konkrétnemu dátumu. V tomto zmysle je legislatíva Českej republiky publikovaná napríklad na súkromnej stránke https://www.zakonyprolidi.cz/ a pre Slovenskú republiku na podobnej stránke https://www.zakonypreludi.sk/. Vzhľadom na praktickosť sú odkazy na národné zákony doplnené aj sekundárnym odkazom na uvedených stránkach. Primárne je ale nutné vychádzať z textu zbierok.

Druhým tematickým okruhom sú štandardy organizácie 3GPP[2], upravujúce požiadavky na mobilné siete tretej a ďalších generácií. Tieto štandardy sú publikované na webovej stránke https://www.3gpp.org/, najmä kvôli pomerne častej aktualizácii a odkazy sú doplnené o URL dokumentov na tejto stránke. Ohľadom štandardizácie mobilných sietí je dokument [6] určitým rozcestníkom a zastrešujúcim štandardom, z ktorého ostatné vychádzajú. Následne dokument [7] identifikuje súbor kritických služieb, pričom technické požiadavky na kritické služby a pre ich fungovanie v mobilných sieťach podrobnejšie rozvádza dokument [8].

1 angl. „Universal Resource Locator“, odkaz na webový zdroj definujúci miesto uloženia tohto zdroja

2 3rd Generation Partnership Project

Ďalšou tematickou časťou sú odborné monografie, ktoré sa venujú témam diskutovaným v práci. Kniha [9] popisuje problematiku diagnostiky technických systémov obecne a je pomerne dobrou učebnicou. Kniha [18] popisuje špecifikáciu požiadaviek, budovanie a praktické overovanie špecializovaného komunikačného systému integrovaného do prostredia letiska, s autonómnymi agentmi. Aj keď to nebol cieľ publikácie, jedná sa o výbornú príručku k budovaniu spoľahlivých špecializovaných informačných a komunikačných systémov. Informácie ku problematike štatistiky a jej využitia ako nástroja pre analýzu a optimalizáciu komunikačných systémov je možné čerpať z [16]. Jedná sa o staršiu, ale kvalitnú odbornú publikáciu. Monografia [12] je venovaná systémovej metodológii, teda obecnému návodu ako pristupovať k akémukoľvek problému konštruktívnym spôsobom a tento nástroj tiež rozvíja pre využitie v rôznych oblastiach ľudskej činnosti. Kniha [10] je určitým centrálnym dokumentom v češtine o analýze a riadení rizík. Autor v nej systematicky popisuje problematiku inžinierstva rizík a uvádza metódy práce s nimi, v prípade tzv. „univerzálnej matice posúdenia rizík“ metódu vlastnú. Aj keď do istej miery sa o to snažila už [10], publikácia [11] inžinierstvo rizík viac posúva k poriadku v terminológii, ktorá často buď chýba alebo je neustálená, pomocou vybudovania terminologického slovníka. Práca popisuje metódu zostavenia slovníka a najmä uvádza výsledky činnosti autorov v siedmych tematických tabuľkách.

Ďalšou tematickou oblasťou sú publikácie Združenia požiarneho a bezpečnostného inžinierstva z edície Spektrum. Jedná sa o sadu tematicky zameraných príručiek z oblasti bezpečnosti, pripravenosti a krízového plánovania. V rámci tejto práce bolo čerpané najmä z [14], ktorá sa venuje ochrane kritickej infraštruktúry od základných princípov, cez analýzu (v čase publikácie) aktuálneho stavu až po metódy identifikácie kritických prvkov a ich ochrany. Ďalej bolo čerpané z [15], ktorá sa venuje bezpečnosti prevádzky technickej infraštruktúry a to najmä rozvodným sieťam elektrickej energie, plynu a pitnej vody, od definície požiadaviek na výstavbu a prevádzku technických infraštruktúr, cez využiteľné prostriedky inžinierstva rizík až po techniky eliminácie nebezpečí hroziacich technickej infraštruktúre.

V oblasti analýzy mobilných sietí nie je možné vynechať časť kľúčových výkonnostných indikátorov. Všeobecný prístup k problematike je rozobratý v monografii [28]. Výborným zdrojom informácií o kľúčových výkonnostných indikátoroch na analýzu a diagnostiku mobilných sietí je súbor dokumentov pozostávajúci z [22] so všeobecným zameraním na mobilné siete, [23] a [24] zameraných na vyvinutú rádiovú prístupovú sieť, [26] pre IP multimediálnu ústredňu IMS (IP Multimedia Subsystem, distribuovaná ústredňa založená na paketovej komutácii, umožňujúca fixnú a mobilnú konvergenciu), [27] zamerané na vyvinuté jadro mobilnej siete a [25] pre rádiovú prístupovú sieť druhej generácie mobilných sietí.

Veľmi dôležitou časťou použitej literatúry sú technické normy vzťahujúce sa k bezpečnosti a metódam analýzy rizík. Jedná sa o normy ČSN, teda České technické normy, ale v tejto problematike ide takmer výlučne o normy prebraté, z časti preto, že technická prax sa bezpečnosti systematicky venovala časovo skôr v zahraničí, ale najmä kvôli medzinárodnej

harmonizácii technickej legislatívy. Norma [13] sa venuje bezpečnosti strojných zariadení a všeobecným zásadám pre ich konštrukciu. Normalizované sú tu postupy pre znižovanie rizika technických zariadení, najmä rizika pre obsluhu. Ďalšie normy sa zameriavajú na konkrétne obecné metódy analýzy rizík technických systémov. Tieto normy popisujú podmienky aplikovateľnosti postupu, ustanovujú formálnu stránku postupu a výstupov a uvádzajú praktické príklady využitia popisovaných metód. V norme [19] je takto popísaná metóda analýzy spôsobov a dôsledkov porúch, v norme [20] zase metóda analýzy stromu udalostí a v norme [21] metóda analýzy stromu poruchových stavov.

Technická referencia výrobcu technológie [17] popisuje praktické aspekty koexistencie viacerých generácií mobilných sietí, kde niektoré, typicky novšie, generácie sa používajú len pre prenos dát, zatiaľ čo pre realizáciu hlasovej služby koncové zariadenie dočasne využíva inú generáciu siete, ktorá podporuje okruhovo spojovaný spôsob komunikácie.

Vzhľadom na interakciu mobilných sietí s ľudskými používateľmi, čo je ich primárny účel, je potrebné čerpať aj z rôznych prieskumov, väčšinou na pomedzí technickej a sociologickej analýzy, študujúcich využitie technológie [29] či analyzujúcich spôsoby využívania služieb používateľmi [30]. Informácie podobného typu je možné tiež nájsť vo výročnej správe ČTÚ (Český telekomunikační úřad) za rok 2020 [31], najmä v častiach venujúcich sa stavu telekomunikačného trhu a odborným činnostiam úradu. Táto kategória zdrojov je všeobecne dostupná len v elektronickej forme.

2 Súčasný stav problematiky

Táto práca vychádza z existujúceho stavu, ktorý sa snaží popísať a navrhnúť voči nemu zlepšenia. Problematiku práce z pohľadu súčasného stavu je možné rozdeliť do niekoľkých častí. Prvou je stav terminológie, pretože sa jedná o medzioborový problém a pretože čiastkový obor inžinierstva rizík nie je zatiaľ terminologicky vymedzený. Druhou analyzovanou časťou je legislatívny rámec, teda národné zákony a smernice rady Európskej únie ako nadnárodného celku, týkajúce sa prevádzky telekomunikačnej kritickej infraštruktúry. Poslednou časťou je súbor medzinárodných noriem ohľadom mobilných bunkových sietí, definujúcich požiadavky na zariadenia, prevádzkové doporučenia a najlepšiu inžiniersku prax.

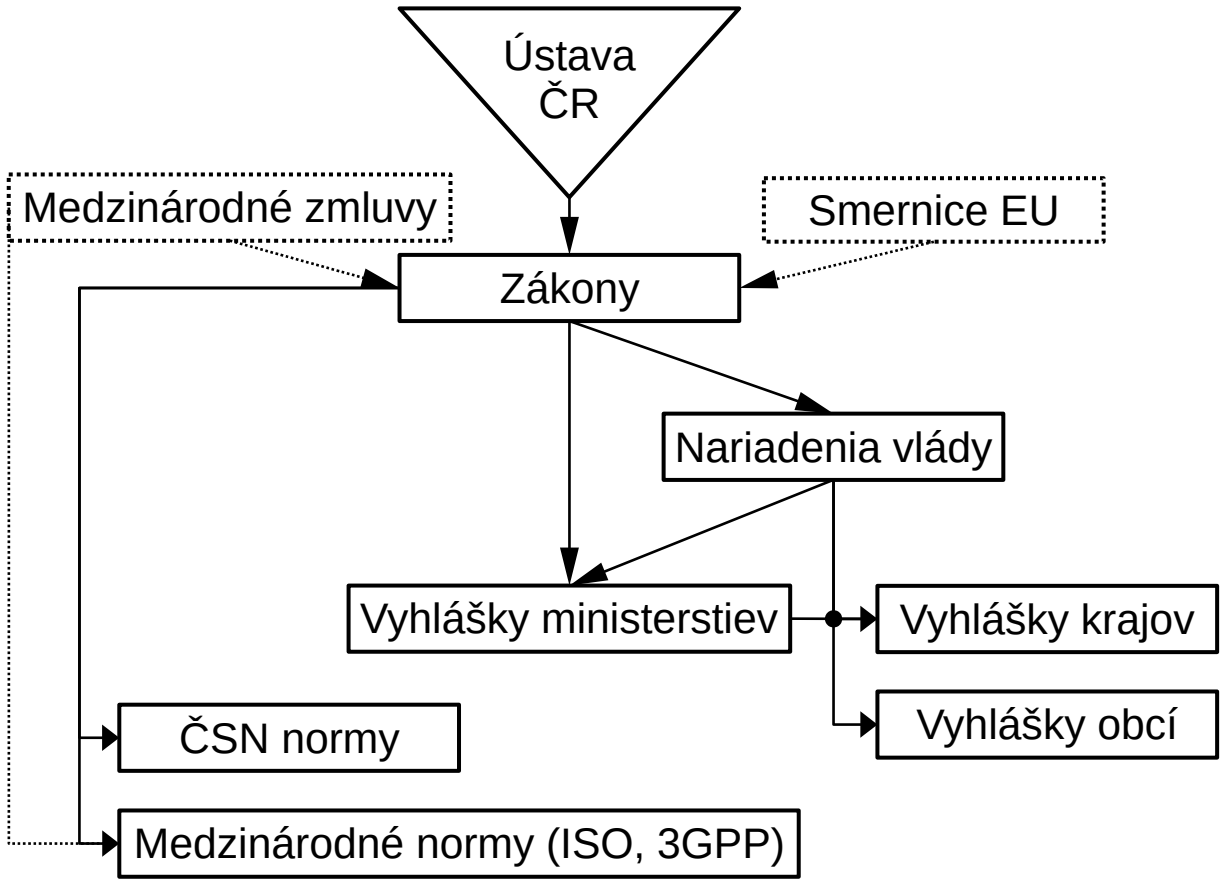
2.1 Terminologické vymedzenie

Vedné disciplíny, ktoré sú vo fáze rozvoja a zatiaľ neprešli ustálením, trpia terminologickým zmätkom. Do tejto kategórie môžeme zarátať aj inžinierstvo rizík. Napriek niekoľkým pokusom o ustálenie terminológie táto stále nie je harmonizovaná naprieč celým oborom, čo vidieť nielen z rôznych publikácií, ako monografií tak vedeckých článkov, ale prejavuje sa to aj v normách.

Z toho dôvodu je nutné väčšinu použitých termínov explicitne definovať a súčasťou práce je ako Príloha č. 1 terminologický slovník. Uvádzaná terminológia a definície z väčšej časti nie sú nové a nie sú dielom autora práce, definované sú pretože ich nemožno považovať za dostatočne ustálené. Pri tvorbe terminologického slovníka sa vychádzalo najmä z troch publikácií, konkrétne „Tichý Milík: Ovládání rizika“ [10] pre oblasť obecnej terminológie rizík, „Procházková Dana a kol.: „Terminologický slovník“ [11] pre oblasť analýzy rizík a „Janíček Přemysl: Systémová metodologie“ [12] pre oblasť systémového prístupu. Ďalšie zdroje pri terminologickom vymedzení slúžili v menšom rozsahu. Jedná sa najmä o definície pochádzajúce z rôznych zákonov vzťahujúcich sa na konkrétne podčasti problému.

2.2 Legislatívny rámec

K problematike fungovania mobilných bunkových sietí ako kritickej infraštruktúry nie sú dostupné žiadne harmonizované normy, ani európske či národné normy a tak je nutné vychádzať z dostupných noriem a doporučení zvlášť pre časť mobilných sietí, a potom zvlášť pre problematiku kritickej infraštruktúry. Existujúce harmonizované normy, ktoré sa venujú bezpečnosti strojných či elektrotechnických zariadení, napr. [13], sú postavené v zmysle bezpečnosti takýchto zariadení pre obsluhu a okolie celkovo (funkčná bezpečnosť). Takýto pohľad je ale v prípade posudzovania kritickej infraštruktúry neaplikovateľný, resp. nevedie k požadovaným výsledkom.



Obr. 1: Štruktúra legislatívnych predpisov v Českej republike, upravené z [15]

Štruktúra legislatívnych predpisov v Českej republike je zobrazená na Obr. 1. Základným legislatívnym dokumentom určujúcim práva a povinnosti osôb v Českej republike je „Ústava České republiky“ [1], kde z pohľadu prevádzky mobilných bunkových sietí v roli kritickej infraštruktúry sú dôležité najmä dva odseky Článku 2, konkrétne ods. 3: „*Státní moc slouží všem občanům a lze ji uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon.*“ a ods. 4: „*Každý občan může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.*“. Podobne pre Slovenskú republiku v „Ústava Slovenskej republiky“ [2], Článok 2, ods. 2: „*Štátne orgány môžu konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon.*“ a ods. 3: „*Každý môže konať, čo nie je zákonom zakázané, a nikoho nemožno nútiť, aby konal niečo, čo zákon neukladá.*“. Tieto koncepty sú dôležité najmä preto, že mobilné bunkové siete operujú na území štátu ako komerčné subjekty v súkromnom vlastníctve a teda štát môže na ich činnosť vplývať len vo forme zákonných nariadení a zároveň ich nemôže priamo „zvýhodňovať“ dotáciami na revitalizáciu kritickej infraštruktúry či na prevenčné opatrenia [14].

Z ústavy vychádzajú zákony, ktoré upravujú konkrétne oblasti fungovania štátu, čo ďalej upravujú nariadenia vlády a vyhlášky ministerstiev, krajov a obcí. Zákony tiež implementujú

požiadavky medzinárodných zmlúv a najmä smerníc EU pre Českú republiku ako členskú krajinu. Poslednou časťou legislatívy sú technické normy, či už národné ČSN alebo prebraté medzinárodné.

2.2.1 Problematika kritickej infraštruktúry

Základnými legislatívnymi dokumentami ohľadom problematiky kritickej infraštruktúry v Českej republike sú Smernica rady Európskej únie 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu [3], ďalej označovaná ako smernica, a implementácia tejto smernice do národného právneho rámca, Zákon č. 240/2000 Sb. - „Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)“ [4], ďalej označovaný ako zákon o krízovom riadení.

Smernica [3] vymedzuje jednotné pojmy pre oblasť krízovej infraštruktúry pre všetky krajiny Európskej únie, poskytuje základné návody k identifikácii kritických infraštruktúr, špeciálne tých európskeho významu, t.j. s cezhraničným dopadom, a pre ich označovanie (informovanie ostatných štátov spoliehajúcich sa na danú kritickú infraštruktúru), definuje potrebu a základné pravidlá pre vytvorenie bezpečnostných plánov a určenie styčných úradníkov (kontaktná osoba na strane prevádzkovateľa kritickej infraštruktúry pre komunikáciu so štátom) a o informovaní ohľadom identifikovaných hrozieb a zraniteľností kritických infraštruktúr smerom ku komisii Európskej rady.

Zákon o krízovom riadení [4] sa zaoberá tzv. stavom nebezpečia, podmienok pre jeho vyhlásenie, úpravou fungovania zložiek štátu a povinnosťami osôb za tohto stavu. Preberá terminológiu definovanú v [3] a určuje orgány krízového riadenia v hierarchickej štruktúre s vymedzením ich právomoci a zodpovednosti pri zaisťovaní pripravenosti štátu na krízové situácie, pri ich riešení alebo pre ochranu kritickej infraštruktúry. Ďalej ustanovuje povinnosti tzv. „subjektov kritickej infraštruktúry“ – prevádzkovateľov takejto infraštruktúry mimo štátnu organizačnú štruktúru, spočívajúce najmä vo vypracovaní plánu krízovej pripravenosti a určení styčných bezpečnostných zamestnancov. Konečne tiež určuje spôsoby kontroly vykonania povinností a postihovania ich nedodržania, ale tiež rámec náhrady škody či obmedzení z uložených krízových opatrení a poskytovania štátnej podpory pri haváriách či živelných pohromách.

Smernica rady EU [3] definuje kritickú infraštruktúru ako „*zložku, systém alebo ich časť nachádzajúcu sa v členských štátoch, ktorá je nevyhnutná pre zachovanie základných funkcií spoločnosti, zdravia, ochrany, bezpečnosti, kvality života obyvateľov z ekonomického a sociálneho hľadiska, a ktorej narušenie alebo zničenie by malo závažné dôsledky v členskom štáte z dôvodu nemožnosti zachovať tieto funkcie*“. Mobilné bunkové siete objektívne sú v dnešnej dobe nevyhnutné pre zachovanie základnej telekomunikačnej funkcie v spoločnosti, všeobecne vzhľadom na trend nahradzovania iných komunikačných zariadení ale aj zariadení

výpočtovej techniky terminálmi mobilných sietí, tiež špeciálne napr. v prípade zníženia mobility v dôsledku núdzového stavu (slovensky „mimoriadnej situácie“). Narušenie či zničenie mobilnej siete by v aktuálne nastavenej spoločnosti malo závažné dôsledky z dôvodu nemožnosti zachovať tieto funkcie. Naviac mobilné bunkové siete sú využívané na komunikáciu okrem civilného obyvateľstva a podnikov do určitej miery aj záchrannými zložkami, čiže ich narušenie by malo vplyv aj na bezpečnostné funkcie. Ďalej je v [3] definovaná európska kritická infraštruktúra ako „*kritická infraštruktúra nachádzajúca sa v členských štátoch, ktorej narušenie alebo zničenie by malo závažné dôsledky minimálne v dvoch členských štátoch. Závažnosť dôsledkov sa posudzuje podľa prierezových kritérií. Toto zahŕňa účinky vyplývajúce z medzisektorových závislostí od iných typov infraštruktúry*“. Jedná sa teda o rozšírenie problematiky kritickej infraštruktúry na cezhraničné dopady. Vzhľadom na hospodárske a sociálne prepojenie krajín v Schengenskom priestore má výpadok komunikačnej infraštruktúry v jednom členskom štáte evidentné dopady na ekonomické a sociálne funkcie štátu a teda mobilná sieť prevádzkovaná na území jedného členského štátu zodpovedá definícii európskej kritickej infraštruktúry. Dôležitým prvkom ktorý sa v definícii európskej kritickej infraštruktúry objavuje je posudzovanie účinkov vyplývajúcich z medzisektorových závislostí od iných typov infraštruktúry, kde smernica prihliada k zmene prevádzkových podmienok a požiadaviek na kritickú infraštruktúru v závislosti na stave ostatných kritických infraštruktúr. Konečne uvedené prierezové kritériá sú definované 3, kritérium straty na životoch, kritérium hospodárskeho vplyvu (straty, zhoršenie výrobkov a služieb) a kritérium vplyvu na verejnosť (dôvera, fyzické utrpenie, narušenie každodenného života) [3]. Dôležitou poznámkou, ktorú [3] uvádza je, že „k*eďže jednotlivé sektory majú špecifické skúsenosti, odborné znalosti a požiadavky v súvislosti s ochranou kritickej infraštruktúry, mal by sa vytvoriť a uplatňovať prístup k ochrane kritickej infraštruktúry na úrovni Spoločenstva, ktorý by zohľadňoval špecifiká jednotlivých sektorov a existujúce sektorovo špecifické opatrenia vrátane tých, ktoré už existujú na úrovni Spoločenstva, na národnej alebo regionálnej úrovni, a prípadne aj cezhraničné dohody o vzájomnej pomoci medzi vlastníkmi/prevádzkovateľmi existujúcich kritických infraštruktúr. Vzhľadom na veľmi dôležitú úlohu súkromného sektora pri kontrole a riadení rizika, plánovaní kontinuity činnosti a obnove po katastrofách má prístup Spoločenstva podporovať plné zapojenie súkromného sektora*“, čiže odporúčanie prihliadať na špecifiká, skúsenosti a zavedenú prax ochrany funkcií kritickej infraštruktúry v danom sektore.

Ďalej smernica [3] definuje potrebu vytvoriť bezpečnostné plány prevádzkovateľa (OSP, angl. „Operator Security Plan“) pre každú európsku kritickú infraštruktúru do jedného roka od identifikácie tejto infraštruktúry, k čomu má kontrolnú úlohu členský štát na území ktorého sa príslušná európska kritická infraštruktúra nachádza. Ohľadom obsahu OSP sa uvádza „*V OSP sa identifikujú zariadenia kritickej infraštruktúry a bezpečnostné riešenia, ktoré existujú alebo sa zavádzajú na ich ochranu.*“ a definujú sa ako minimálna náplň OSP: identifikácia dôležitých zariadení, vykonanie analýzy rizika na základe scenárov hrozieb, zraniteľností a možných

dôsledkov a identifikáciu a prioritizáciu nápravných opatrení kde sa rozlišuje skupina stálych opatrení (zameraná na informovanie, vzdelávanie a budovanie správnej technickej praxe a výberu vhodných technických, kontrolných, komunikačných a overovacích postupov) a odstupňovaných postupne aktivovaných v závislosti na realizovaných rizikách.

K naplneniu uvedených požiadaviek je prisľúbená podpora nasledovne: *„Komisia prostredníctvom príslušného orgánu členského štátu podporuje vlastníkov/prevádzkovateľov označených ECI*[3] *takým spôsobom, že im sprístupní dostupné najlepšie postupy a metodiky, ako aj podporné odborné vzdelávanie a umožní výmenu informácií o najnovšom technickom vývoji v oblasti ochrany kritickej infraštruktúry.“* [3], ale bez ďalších informácií ako sa k prisľúbeným zdrojom dopracovať.

2.2.2 Problematika kybernetickej bezpečnosti

Na mobilné siete sa v ČR aplikuje tiež Zákon č. 118/2014 Sb. [5], t.j. zákon o kybernetickej bezpečnosti, pretože podľa tohto zákona sa mobilná sieť považuje za komunikačný systém kritickej infraštruktúry. Vymedzenie v zákone [5] je nasledovné: podľa §2 písm. b) sa rozumie *„kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti*“ a podľa §3 písm. c) sa správcovi a prevádzkovateľovi kritickej informačnej infraštruktúry ukladajú podľa tohto zákona povinnosti popísané ďalej.

Zákon [5] definuje kybernetickú bezpečnostnú udalosť v §7 bode (1) *„Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací*“ a kybernetický bezpečnostný incident v §7 bode (2) *„Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události*“. Podľa §7 bodu (3) sa ukladá správcom a prevádzkovateľom povinnosť detekovať kybernetické bezpečnostné udalosti v ich významnej sieti, informačnom či komunikačnom systéme a podľa §8 povinnosť hlásiť kybernetické bezpečnostné incidenty prevádzkovateľovi národného CERT (angl. „Computer Emergency Response Team“, tím reakcie na počítačové krízové situácie) a úradu zodpovednému za kybernetickú a informačnú bezpečnosť. Ďalej [5] upravuje povinnosti počas stavu kybernetického nebezpečia, definovaného v §21 bode (1): *„Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací*“, ktorý podľa ďalších

3 European Critical Infrastructure, európska kritická infraštruktúra

bodov tohto paragrafu vyhlasuje úrad pre kybernetickú a informačnú bezpečnosť a počas trvania tohto stavu koordinuje aktivity pre jeho potlačenie a informuje nadriadený orgán, vládu ČR o postupoch riešenia.

V §4 zákona [5] je definovaný systém zaistenia kybernetickej bezpečnosti na základe bezpečnostných udalostí v bode (1): „*Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru*“.

Ostatné ustanovenia zákona sa týkajú povinností orgánov štátnej správy v procese zachovania kybernetickej bezpečnosti a do povinností súkromných a právnických osôb vstupujú len málo.

2.2.3 Problematika prevádzky mobilných sietí

Z oblasti doporučení pre výstavbu a prevádzku mobilných sietí, toto zastrešuje organizácia 3GPP od ich tretej generácie, ktorá bola prvá celosvetovo koordinovaná, ďalej. Terminológia zavedená v rámci 3GPP ohľadom kritickej infraštruktúry hovorí o tzv. kritických službách (angl. „mission critical services“), teda službách na možnosti realizácie ktorých sa spolieha nejaká verejná služba (poriadkové sily, zdravotná služba, hasičský a záchranný zbor), či iná kritická infraštruktúra (energetika). Definovanie platformy pre kritickú komunikáciu si 3GPP určila za kľúčový cieľ a tento postupne napĺňa od Vydania 13 (angl. „Release 13“)[4], kde bola pridaná podpora pre kritickú verziu služby push-to-talk („vysielačkový“ režim komunikácie s veľmi krátkou dobou nadviazania spojenia, vrátane skupinovej komunikácie). V R14 bola pridaná podpora pre kritické dátové prenosy a kritické videoprenosy. Vydanie R15 sa zameriavalo na zlepšenie interoperability kritických služieb a tiež začalo integrovať požiadavky špecifické pre konkrétne typy kritickej transportnej infraštruktúry, konkrétne železničnej a námornej dopravy. [7]

Centrálnym dokumentom 3GPP k problematike kritických služieb je [8], ktorý definuje spoločné požiadavky na kritické služby „vysielačkového“ prenosu hlasu, prenosu dát a videotelefónie tak, aby boli použiteľné pre zabezpečenie verejne bezpečnostných služieb, ale tiež mobilných telekomunikačných potrieb komerčných kritických infraštruktúr. Toto doporučenie sa ale vzťahuje len na siete 4G a ďalších generácií[5]. Pre fungovanie komunikačného systému v roli kritickej infraštruktúry je potrebné, aby komunikácia prebiehala spoľahlivo nie len v núdzovom stave, ale samozrejme aj za bežných podmienok. Systém štandardov 3GPP pomerne podrobne definuje chovanie jednotlivých prvkov a postup signalizačných a riadiacich procedúr. Aj keď

4 3GPP aktuálne používa systém paralelne platných vydaní, čo sú na vlastnosti orientované zmrazené body vývoja k určenému dátumu, s vodopádovým modelom, kde ďalší vývoj a nové vlastnosti sú smerované do nasledujúcich vydaní. Aktuálne vydanie je Release 16. Podrobnejšie informácie v [6].

5 V 2G (GSM) a 3G (UMTS) bolo možné použiť okruhovo prepínaný spôsob komunikácie, s nízkou latenciou a jej kolísaním, ktorý bol od 3,9G vynechaný a teda je potrebné parametre kritických služieb zabezpečiť špeciálne.

v systémoch sieťovo organizovaných je možné identifikovať prvky a prepojenia ktoré sú pre funkciu celku dôležitejšie ako iné, žiadny prvok či spoj typicky nebýva zbytočný. Vzhľadom k tomu je celé pemzum štandardov 3GPP určitým spôsobom potrebné pre prevádzku mobilných sietí v roliach kritickej infraštruktúry. Dokument [6] je rozcestníkom, z ktorého je možné sa dostať k špecifikácii konkrétneho prvku, rozhrania či služby podľa vydania ktorému má zodpovedať a zaradenia v štruktúre mobilnej siete.

2.3 Zhrnutie kapitoly

V tejto kapitole bol sumarizovaný aktuálny stav problematiky mobilných bunkových sietí vo funkcii kritickej infraštruktúry. Pretože neexistuje ucelená legislatíva na túto tému, je potrebné vychádzať z čiastkových legislatívnych dokumentov a nájsť ich prienik či harmonizáciu medzi nimi. Vzhľadom na roztrieštenosť terminológie sa takéto zbližovanie začína snahou o ustálenie terminologického slovníka. Výsledok tejto činnosti je uvedený v prílohe č. 1. Ďalším krokom, z ktorého ale budovanie terminologického slovníka tiež čerpá, je analýza legislatívy vzťahujúcej sa k problematike. Okrem základných právnych predpisov (ústavy) je to najmä tzv. zákon o krízovom riadení [4], ktorý popisuje kritickú infraštruktúru, postupy jej správy a zabezpečovania pripravenosti na mimoriadne situácie. Ďalej sa k prevádzke mobilných sietí ako systému elektronickej komunikácie viaže zákon o kybernetickej bezpečnosti [5], ktorý popisuje povinnosti prevádzkovateľa pri narušení dostupnosti služby či dôvernosti a integrity dát.

Technická prevádzka mobilných sietí je normalizovaná v dokumentoch 3GPP, čo je súbor dokumentov popisujúcich požiadavky, odporúčania a postupy pre mobilné siete a ich jednotlivé súčasti. Tieto dokumenty popisujú komplexnú problematiku mobilných sietí štruktúrovane a previazane, na fungovanie mobilných sietí ako kritickej infraštruktúry sa ale dajú aplikovať len niektoré z nich.

Na uvedených analyzovaných legislatívnych dokumentoch je možné ďalej stavať a využiť ich pri nadväzujúcej systematickej práci na téme, k čomu dávajú dostatočný základ.

3 Ciele práce

Primárnym cieľom práce, definovaným v originálnom zadaní, je vykonanie analýzy rizík pre posúdenie možností prevádzky mobilnej bunkovej siete v roli kritickej infraštruktúry. Tento cieľ má dve čiastkové časti a to posúdenie mobilnej siete ako chráneného aktíva a ako zdroja ohrozenia.

Čiastkovými cieľmi, podporujúcimi dosiahnutie primárnych cieľov, sú:

- popis a diskusia metód práce s rizikami z oblastí inžinierstva a riadenia rizík pre využitie k analýze rizík mobilných sietí a prevádzku mobilných sietí ako kritickej infraštruktúry,
- analýza metód diagnostiky mobilných sietí vyplývajúcich z priemyselnej praxe odvetvia mobilných bunkových telekomunikácií,
- podrobný popis mobilnej siete na základe systémového prístupu, teda zameraný na jednotlivé prvky, vzťahy medzi nimi a s okolím systému,
- praktické overenie vybudovanej teoretickej štruktúry pre podporu mobilných sietí v roli kritickej infraštruktúry na reálnych mobilných sieťach komerčných operátorov.

Ďalšími sekundárnymi cieľmi, vychádzajúcimi zo zadania, sú:

- zameranie analýzy možností realizácie funkcií kritickej infraštruktúry mobilnou sieťou ako za bežnej prevádzky, tak v prípade mimoriadnych udalostí či stavu nebezpečia,
- vykonanie diskusie technických a organizačných opatrení pre ochranu funkcií kritickej infraštruktúry v mobilných sieťach.

Tieto ciele, tak ako sú vyššie definované, sú postupne napĺňané v nasledujúcich kapitolách a dosiahnuté výsledky zhrnuté v závere práce.

4 Použité metódy

Pre analýzu a následne riešenie problému prevádzky mobilných bunkových sietí ako kritickej infraštruktúry je možné využiť viacero metód, ktoré sú diferencovateľné na základe spoločných charakteristík do niekoľkých skupín. Prvou takouto skupinou sú metódy analýzy rizík technických systémov, vychádzajúce z oblasti obecného inžinierstva rizík. Druhou skupinou metód sú metódy diagnostiky mobilných sietí, vychádzajúce z priemyselnej praxe a aplikovaného výskumu v oblasti prevádzky mobilných bunkových sietí. Tieto dve časti sú doplnené podpornými metódami ako je popisná štatistika a tiež súbor kľúčových výkonnostných indikátorov, využiteľných u mobilných sietí pre hodnotenie funkcie a porovnanie.

4.1 Metódy analýzy rizík technických systémov

Inžinierstvo rizík ako vedný obor za dobu svojej existencie prišlo s niekoľkými metódami analýzy rizík, či už kvalitatívnymi, tak kvantitatívnymi. Tieto metódy pomáhajú na zodpovedajúcej a často voliteľnej úrovni detailov a rozsahu identifikovať hrozby a zraniteľnosti objektov rizika, kvalifikovať a vo vybraných prípadoch kvantifikovať mieru rizika, prípadne navrhnúť a kvantifikovať náklady a dopady bezpečnostných opatrení pre zmiernenie rizika. Existujúce metódy majú svoje slabé a silné stránky, nie je možné jednoznačne určiť ktorá z nich je lepšia globálne [14], pričom niekedy je takéto zoradenie problematické aj v konkrétnych prípadoch. Výsledok vhodnej metódy musí pokrývať analyzovaný objekt dostatočne komplexne, musí reprezentovať reálne a na zvolenej úrovni riešiteľné riziká a hlavne musí byť zrozumiteľný okrem odbornej verejnosti aj laikom, pretože funkčné riadenie rizík vyžaduje zapojenie všetkých osôb ktoré s objektom rizika interagujú či prichádzajú do kontaktu. Nasleduje popis niektorých metód analýzy rizík technických systémov a diskusia ich využiteľnosti v problematike mobilných sietí.

4.1.1 Analýza spôsobov a dopadov porúch (FMEA)

Metóda FMEA (angl. „Failure Mode and Effect Analysis“, analýza spôsobov a dopadov porúch), definovaná v norme [19], je analytický postup založený na rozbore spôsobov vzniku porúch a ich dôsledkov, umožňujúci hľadanie dopadov a príčin štruktúrovane. Jedná sa o metódu často používanú a jednu z prvých volieb pre analýzu rizík kvôli svojej relatívnej jednoduchosti ale v porovnaní s tým s celkom dobrými výsledkami. Metóda je tiež dostatočne všeobecná, ide často aplikovať na ľubovoľný proces, postup, zariadenie či systém zariadení. Pre zjednodušenie využitia metódy týmto univerzálnym spôsobom existujú viaceré varianty a to konkrétne varianta systémová, ktorá umožňuje analyzovať funkčnú súčinnosť (interoperabilitu) prvkov komplexného systému a ich vzájomné interakcie; ďalej varianta konštrukčná, zameraná na

identifikáciu a preverenie potenciálnych chýb počas návrhu, konštrukcie, dimenzovania, výroby či montáže zariadenia; a konečne procesná varianta pre identifikáciu zdrojov chýb počas procesu, primárne výrobného, obecne ľubovoľného. O rozšírenosti svedčí aj to, že metóda je popísaná vo viacerých prehľadových literárnych zdrojoch v práci použitých, teda okrem normy vyššie konkrétne [10] a [14].

Formálne sa pri metóde FMEA vytvára tabuľka spôsobov porúch prvkov systému a ich dopadov na skúmaný systém či proces. Poruchový stav definuje spôsob zlyhania, teda z akého východzieho stavu a akým spôsobom dôjde k zlyhaniu. Dopad poruchy je ovplyvnený reakciou analyzovaného systému na poruchu prvku. Metódou FMEA je možné identifikovať najmä jednoduché poruchy, ktoré priamo vedú k nehode alebo k nej prispejú výrazným spôsobom, príliš dobre ale neumožňuje analyzovať nehody spôsobené kombináciou viacerých porúch. [14]

Metóda FMEA umožňuje tvorbu doporučení pre zvýšenie spoľahlivosti zariadenia či zlepšenie bezpečnosti procesu. Vykonáva tiež vyhodnotenie dopadov najhoršieho prípadu plynúceho z identifikovaných porúch a návrhy nápravných opatrení. Výsledky sa ľahko aktualizujú pri zmenách. Metóda FMEA je vhodnou zastrešujúcou analýzou rizík prvého sledu, s neskorším zaradením ďalších analýz.

V prípade mobilných sietí je metóda FMEA taktiež vhodnou počiatočnou metódou pre získanie prehľadu o možných poruchách. Je možné ju vykonávať aj nad všeobecným modelom mobilnej siete, nie len nad konkrétnou sieťou a teda je možným zdrojom položiek do kontrolného zoznamu – kap. 4.1.7.

4.1.2 Analýza stromu udalostí (ETA)

V prípade metódy ETA (angl. „Event Tree Analysis“, Analýza stromu udalostí), definovanej v norme [20], sa jedná o sledovanie procesov od ich iniciačnej udalosti pomocou binárneho vyhodnocovania priaznivých a nepriaznivých možností vývoja v jednotlivých ich fázach. Takýmto postupom vzniká graf ktorý sa v každom kroku vetví s jednotlivými udalosťami v pozorovanom procese. Táto metóda je vhodná na sledovanie spoľahlivosti procesov, postupov a procedúr. Výsledkom ETA je scenár realizácie rizika a súbor zlyhaní, ktoré vedú k nežiadúcej udalosti. Metódu je možné aplikovať aj v kvantitatívnom režime, kedy sa postupným krokom priradia pravdepodobnosti variantov a možné koncové stavy sú následne aj pravdepodobnostne ohodnotené. Pre použitie metódy ETA je nutné identifikovať množinu možných iniciačných udalostí procesov ktoré sa majú skúmať a následne je potrebná podrobná znalosť analyzovaných procesov, kvôli ich dekompozícii na čiastkové udalosti. V prípade kvantitatívnej varianty sú potrebné merania relatívnej početnosti alebo iné odhady pravdepodobnosti variantov v jednotlivých krokoch [14].

Norma [20] špecifikuje základné princípy analýzy stromu udalostí, postup pre modelovanie následkov iniciačnej udalosti a ich vyhodnotenie v kontexte spoľahlivosti a rizika.

Pre tento účel sú tam určené procedurálne kroky metódy, postup vypracovania predpokladov, obmedzení a prínosov využitia metódy ETA a previazanosť s inými metódami analýzy rizík a kvantifikácie spoľahlivosti technických systémov.

V praxi sa výsledky metódy ETA používajú pre identifikáciu slabých miest projektov či procesov a následný návrh doporučení pre zníženie pravdepodobnosti udalostí či ich dopadov. Stromy udalostí sa väčšinou používajú pri zložitých procesoch. Je možná kombinácia metódy ETA s metódou FTA (kapitola 4.1.3), kde z nehodových sekvencií vytvorených metódou ETA sú pomocou metódy FTA určené typické kombinácie zlyhaní k nim vedúcich, čo vedie na množiny úspechov či neúspechov bezpečnostných systémov náležiacich k možným koncovým stavom.

V prípade mobilných sietí je metóda ETA aplikovateľná napríklad aj na jednotlivé signalizačné procedúry, kde je pomocou nej možné identifikovať možné poruchy a zlyhania v týchto procedúrach a koncové chybové stavy pomerne dobre reprezentujúce symptómy zlyhania.

4.1.3 Analýza stromu porúch (FTA)

Metóda FTA (angl. „Fault Tree Analysis“, analýza stromu porúch), definovaná v norme [21], je založená na systematickom spätnom rozbore udalostí v príčinnom reťazci definovanej vrcholovej udalosti, zobrazuje strom porúch v grafickej forme rozvetveného grafu. Zmyslom tejto metódy je posúdenie pravdepodobnosti vzniku vrcholovej udalosti s využitím analytických alebo štatistických metód. Výstupom je súbor možných technických a ľudských chýb vedúcich k špecifikovanej nežiadúcej udalosti a ich vzájomné vzťahy a závislosti. Metóda FTA je vhodná pre analýzu rozsiahlych a zložitých systémov či zariadení u ktorých nie sú známe časté zraniteľnosti voči konkrétnym hrozbám. Táto metóda sa tiež často používa pre detailnejšiu analýzu vážnych hrozieb identifikovaných inými metódami, keďže umožňuje vytvorenie logického modelu poruchy zariadenia založeného na booleovskej algebre. Na základe viacerých týchto modelov pre rôzne vrcholové udalosti sa vytvárajú tzv. „minimálne kritické rezy“, čo sú skupiny udalostí vedúcich ku konkrétnej poruche, pričom kritické rezy obsahujúce viac čiastkových porúch sú z definície menej rizikové.

Identifikované kombinácie základných porúch zariadení a ľudských chýb potenciálne vedúcich k nehode umožňujú zameranie na opatrenia preventívne či zmierňujúce dopady u významných základných príčin ekonomicky výhodným spôsobom [14]. Metóda FTA vychádza z následkov možnej chyby, vedúcej k nežiadúcemu javu a vyšetruje príčiny tohto stavu.

Metóda FTA sa v priemyselnej praxi využíva k trom účelom. Počas projektovania technického zariadenia umožňuje identifikovať nežiadúce stavy systému a teda slúži k preventívnemu zabezpečovaniu akosti. V procese rozhodovania umožňuje vybrať optimálnu variantu riešenia a teda slúži k overeniu koncepcie systému. V prípade výskytu chyby počas prevádzky či výroby umožňuje identifikovať jej zdroje a teda sa jedná o nástroj technickej

diagnostiky a riešenia problémov. Výhodne je využitie metódy pre vyhodnotenie bezpečnosti zložitých štruktúr s mnohými prvkami či rozľahlých systémov, ako sú dopravné systémy či elektrárne. Vyskytuje sa ale aj využitie pre analýzu pohotovosti či udržateľnosti.

Norma [21] popisuje kroky analýzy FTA, teda vymedzenie základných princípov a následnú identifikáciu udalostí a spôsobov porúch. Popísaný proces sa zaoberá identifikáciou a analýzou podmienok a faktorov, ktoré buď spôsobujú alebo potenciálne môžu spôsobiť výskyt alebo prispieť k výskytu analyzovanej vrcholovej udalosti. Vrcholovou udalosťou je obvykle porucha, poruchový stav, zhoršenie fungovania analyzovaného systému, zníženie bezpečnosti či zhoršenie iných dôležitých prevádzkových parametrov.

U mobilných sietí je metóda FTA použiteľná najmä v jej variante pre hľadanie možných príčin identifikovaného chybového stavu. Takýto stav môže byť zachytený pracoviskom riadenia kvality a odovzdaný pre analýzu technickému oddeleniu. Iné metódy, vychádzajúce zo zvyklostí odvetvia, popísané v kap. 4.2, ale často poskytnú rovnaký výsledok v kratšom čase. Zmysluplnejšie sa teda javí využitie metódy FTA pri projektovaní prvkov, čo ale nespadá do kompetencie prevádzkovateľa siete.

4.1.4 Analýza príčin a dopadov (CCA)

Metóda CCA (angl. „Causes and Consequences Analysis“, analýza príčin a dopadov) je kombináciou dvoch predchádzajúcich analýz, FTA a ETA. Podobne ako metóda FMEA sa zaoberá príčinami a možnými dopadmi analyzovanej entity. Je veľmi citlivá na voľbu úrovne detailov, pretože výsledný graf sa ľahko môže stať neprehľadným. Výstupom je diagram priebehu nehody s kvalitatívnym popisom možných koncových stavov.

Metóda CCA je pomerne náročná na znalosti o analyzovanom systéme [14]. Pre jej vykonanie sú potrebné detailné informácie o možných poruchách jednotlivých prvkov systému, ktoré by mohli viesť k nehode, prípadne pre analýzu procesov podobné znalosti o slabých miestach procesu. Ďalej je nutná dobrá znalosť existujúcich bezpečnostných postupov, ktoré sa na analyzovaný problém aplikujú a tiež spúšťacie mechanizmy a priebeh funkcie bezpečnostných systémov, pretože v časti pokrytej metódou ETA tieto výrazne ovplyvňujú dosiahnuteľné koncové stavy a pravdepodobnosti ich dosiahnutia. V neposlednom rade je potrebná znalosť všetkých potenciálnych efektov možných zlyhaní. V ohľade požiadaviek na predchádzajúce znalosti o systéme teda kombinuje nevýhody metód ETA a FTA.

V praxi sa táto metóda používa najmä pre účely dokumentácie, kedy výsledný diagram zobrazuje vzťahy medzi koncovými stavmi a ich základnými príčinami. Pre skutočnú analýzu rizík je použiteľná len v prípade, keď je logický sled od porúch k nehodám jednoduchý.

V prípade mobilných sietí je metóda CCA použiteľná najmä na dokumentáciu procedúr a vývoja ich možných chybových stavov, k tomuto účelu je ale väčšinou vhodnejšia metóda komunikačného diagramu.

4.1.5 Univerzálna matica rizikovej analýzy (UMRA)

Metóda UMRA (Univerzálna matica rizikovej analýzy, angl. „Universal Matrix of Risk Analysis“), popísaná autorom v [10], je dvojfázová metóda pre analýzu rizika, tabuľkovo formalizovaná. Prvá fáza je zameraná na identifikáciu častí analyzovaného projektu či procesu vystavených nebezpečiam a zdrojov nebezpečí ktoré tieto časti ohrozujú. V druhej fáze sa z aspektov identifikovaných vo fáze prvej vytvorí matica a ohodnotia sa interakcie, čo predstavuje odhad závažnosti. Autor metódu popisuje ako založenú na logicko-numerickej analýze závažnosti nebezpečia pre vyšetrovaný projekt.

Metóda UMRA vznikla pre posudzovanie stavebných projektov[6], je ale postavená dostatočne všeobecne, aby bola použiteľná aj mimo túto oblasť. Kladie veľký dôraz na rolu expertov v posudzovaní a umožňuje efektívne spracovať výsledky veľkého tímu, no priznáva im aj predpojatosti a rozdiely vo vnímaní úrovne nebezpečia, ktoré sa snaží korigovať na základe matematických postupov.

Logicky metóda rozdeľuje faktory na segmenty, čo sú vlastnosti či časti analyzovanej entity a zdroje, čo sú zdroje nebezpečia. Pre segmenty požaduje len existenčnú či sekvenčnú závislosť a zakazuje závislosť fyzikálnu, nesmú obsahovať iné segmenty či byť ďalej deliteľné. Podobne zdroje ohrozenia nesmú byť ďalej deliteľné ani obsahovať iné zdroje a dovoľuje sa u nich len existenčná závislosť. Pre posudky expertov sa vypočítavajú individuálne súčinitele vnímania nebezpečia, následne z nich súčiniteľ tímový. Výsledky expertov a tímu sa korigujú na základe týchto hodnôt. Metóda explicitne uvádza, že výsledky jedného tímu nie sú porovnateľné s výsledkami inak zložených tímov expertov. [10]

V prípade mobilných sietí je metóda dobre využiteľná v úlohe prehľadovej analýzy, kedy sa vykoná segmentácia analyzovaného procesu či zariadenia, identifikujú sa možné zdroje ohrozenia, zostaví sa matica a ohodnotia sa interakcie medzi segmentami a zdrojmi ohrozenia. Z týchto hodnôt je dobre viditeľné, ktorým častiam (segmentom) a na druhú stranu ktorým zdrojom ohrozenia je potrebné venovať pozornosť. Metóda je použiteľná aj individuálne, s rastúcim počtom expertov ale stúpa jej výpovedná hodnota.

4.1.6 Analýza ľudskej spoľahlivosti (HRA)

Metóda HRA (angl. „Human Reliability Analysis“, analýza ľudskej spoľahlivosti) je zameraná na systematickú analýzu príčin a dôsledkov zlyhaní ku ktorým prispieva ľudský faktor v socio-technických systémoch. Pri analýze sa využíva mikroergonomický princíp pre posudzovanie interakcie človeka a stroja a makroergonomický princíp pre posudzovanie interakcie človeka s technológiou ako celkom. Pri analýze je nutné vychádzať z platných predpisov o bezpečnosti a

6 Prvý krát bola použitá pre odhad nebezpečí pri budovaní trasy metra C popod rieku Vltava. Je zameraná najmä na prácu s nebezpečiami, čím sa mierne odlišuje od ostatných metód.

ochrane zdravia pri práci. Metódu je vždy nutné kombinovať s inými metódami pre posúdenie rizík čisto technickej povahy. [14]

Analýza ľudskej spoľahlivosti sa zameriava na faktory ovplyvňujúce výkonnosť operátorov zariadení, technikov a ostatného personálu. Pre úspešné vykonanie vyžaduje u posudzovateľa ako znalosti pracovných postupov, charakteristík a rozloženia prostredia výkonu konkrétnej práce a spôsobu signalizácie a ovládania zariadení, tak požiadaviek na vedomosti, schopnosti, znalosti a praktické skúsenosti obsluhy. Výsledkom analýzy je zoznam situácií náchylných na ľudské chyby či omyly, ktoré kvôli nim môžu viesť k nehodám, so zameraním na príčiny týchto pochybení. Pri analýze je možné sa venovať zvlášť rôznym režimom prevádzky, napr. normálnemu, chybovému či núdzovému a posudzovať zdroje chýb v týchto situáciách. Takéto výsledky sú tiež dobrým podkladom pre tvorbu bezpečnostných opatrení na zmiernenie rizika.

Analyzované priestupky u osôb sa rozdeľujú na: neznalosť ako dôsledok nedostatočného vzdelania či informovania, neskúsenosť ako špecifická forma neznalosti, nedbalosť ako nevhodný prístup k práci, omyl ako dôsledok neúplnosti či nesprávnosti informácie pri rozhodovaní, chyba ako náhodné zlyhanie spôsobené nepozornosťou, zlozvyk ako nesprávna skúsenosť, zlý úmysel ako uprednostnenie vlastného úžitku pred profesionálnym, dobrý úmysel kombinovaný s neodbornosťou a konečne mimoriadne okolnosti ovplyvňujúce stav a uvažovanie človeka [10].

V prípade mobilných sietí je analýza HRA využiteľná najmä pre identifikáciu oblastí náchylných na chybu obsluhy špeciálne tam, kde neboli vykonávané procesy automatizované. Jedná sa najmä o prácu technikov pri fyzických inštaláciách a údržbe, ale taktiež o akékoľvek špecializované a málo časté úkony s potenciálom vážnych nehôd či obmedzenia funkcie po dlhšiu dobu.

4.1.7 Kontrolný zoznam

Metóda kontrolného zoznamu (angl. „checklist“) je postup založený na systematickej kontrole plnenia dopredu stanovených zoznamov podmienok a opatrení. Tieto zoznamy vychádzajú z charakteristík sledovaných systémov či súvisiacich procesov a dopadov realizácie možných nebezpečí. Základom je porovnanie stavu analyzovaného systému či procesu so stavom požadovaným či predpokladaným. V zložitejších formách môžu mať jednotlivé položky priradenú váhu, či je možné vetvenie na základe stavu položky. Je nimi možné pokryť celý životný cyklus systému či procesu a sú tiež vhodným nástrojom pre rozhodovanie, špeciálne ak je nutné rozhodnutie vykonať v krátkom čase. Metóda je efektívna pri odhadovaní sekundárnych a ďalších rádov dopadov či vzťahov medzi dopadmi. Tiež pomáha odhaľovať problémy pre následné podrobnejšie analýzy. Dá sa s výhodou využiť aj pre oboznámenie neskúseného personálu s procesom či zariadením. [14]

Kontrolné zoznamy sa často využívajú pri projektovaní, inštalácii a činnostiach ďalších, buď zriedkavo vykonávaných alebo vyžadujúcich presné dodržanie operačných podmienok. Na druhú stranu sú pomerne jednoduché na vykonanie a kladú malé nároky na odbornosť a znalosti kontrolujúcej osoby, väčšie už na svedomitosť. Ťažisko odbornosti sa presúva na autora, kde sú zase nároky pomerne vysoké, ideálna je preto ich tvorba v, podľa možností heterogénnom, tíme. Je tiež nutné ich priebežne aktualizovať, inak rýchlo strácajú na užitočnosti a stávajú sa skôr prekážkou bezpečnosti procesu, ktorú mali podporovať.

V prípade mobilných sietí sú kontrolné zoznamy široko aplikovateľné v akýchkoľvek situáciách, kde činnosti vykonáva menej skúsená či odborne pripravená osoba ako metóda včasného odhalenia a predchádzania rizikám. Pri odborných činnostiach a diagnostike naopak príliš užitočné nie sú kvôli typickej neopakovateľnosti situácie či nemožnosti jednoduchého zistenia odchýlky od normálneho stavu.

4.1.8 Diagram rybacej kosti

Diagram rybacej kosti alebo tiež Ishikawov diagram príčin a následkov je jednoduchý druh štruktúrovanej analýzy rizík technických systémov založený na posudzovaní ôsmych aspektov potenciálu poruchy, menovite: ľudí, metód, nástrojov, materiálu, merania, prostredia, riadenia a údržby. Formálne sa vychádza z vrcholovej udalosti, čo je analyzovaná porucha, zlyhanie či neúspech procesu, kde sa následne hľadajú možné zdroje vo vyššie uvedených ôsmych kategóriách, kde identifikované príčiny sú ďalej analyzované, aby sa našli ich možné predchádzajúce príčiny a značené ako nadväzujúce výhonky vo fraktálnej konfigurácii. Jednotlivé úrovne zanorenia sú teda v hierarchickej príčinnej súvislosti ku svojmu nadradenému výhonku.

Metóda je využiteľná podobným spôsobom ako FTA (kap. 4.1.3), ohľadom výsledkov je porovnateľná len s jej kvalitatívnou verziou, ale formálne vo jednoduchšej a v kompaktnejšej forme. Výhodou diagramu rybacej kosti je, že počas jej vykonávania či po skončení je možné jasne vizuálne identifikovať oblasti, ktoré neboli dostatočne analyzované, pretože je u nich menšie vetvenie či plytkejšie zanorenie[7].

Využitie pri analýze mobilných sietí je najmä ako rýchlej náhrady FTA pre tímovú analýzu konkrétneho zlyhania, ktorého príčiny sa nepodarilo odhaliť pomocou exploratórneho využitia diagnostických metód. Pre identifikované možné príčiny je následne možné vytvoriť diagnostický plán a preveriť ich cieleným meraním.

7 V grafe je viditeľné „prázdne miesto“.

4.1.9 Metódy analýzy ekonomických rizík

Prevádzkovateľ mobilnej siete je komerčný subjekt. Prevádzku siete ako technického systému teda okrem technických rizík ohrozujú aj riziká ekonomické. Riadenie ekonomických rizík je mimo tému tejto práce, preto sú používané postupy a metódy v nasledujúcom texte charakterizované len stručne. Vo všeobecnosti sa s ekonomickými rizikami vo firmách začína pracovať výrazne skôr ako s rizikami technickými, pretože sú bližšie riadiacim pracovníkom, a tak v dobe keď sa z prevádzkovaného systému stáva kritická infraštruktúra je ekonomický stav prevádzky väčšinou dostatočne zabezpečený. Život firmy ale vyžaduje realizáciu zmien pre prispôsobenie sa zmeneným podmienkam a tieto zmeny sú zdrojom neistoty a možných hrozieb aj pre technickú infraštruktúru.

Posudzovanie ekonomických rizík ohrozujúcich firmu sa tiež nazýva strategickou analýzou firmy a rozumie sa tým postup pre objasnenie faktorov, interných aj externých, podmieňujúcich úspech firmy. Takáto analýza je vykonávaná najmä za účelom identifikácie dôvodov existujúceho nežiadúceho stavu a návrhu nápravných opatrení. Druhou častou funkciou strategickej analýzy je teda ohodnotenie možnosti realizovať potrebnú zmenu, napr. v spôsobe komunikácie, riadenia či správy aktív.

Prvým krokom strategickej analýzy firmy je posúdenie vnútorných faktorov firmy, k čomu je možné použiť napr. metódu 7S vyvinutú konzultačnou firmou McKinsey. Jedná sa o metódu pri ktorej sa podrobne rozoberajú oblasti ako hierarchia stratégií a cieľov firmy, jej organizačná štruktúra, jednotliví spolupracovníci a ich schopnosti, štýl riadenia, komunikačné systémy a firemná kultúra. Detailný popis jednotlivých oblastí je následne vstupom pre metódu posúdenia, napr. SWOT (angl. „Strengths, Weaknesses, Opportunities, Threats“, analýza silných a slabých stránok, hrozieb a príležitostí). Cieľom analýzy McKinsey 7S je odpovedať na otázku či je firma vnútorne pripravená na plánovanú zmenu. Tiež je vhodné sa zamerať na identifikáciu možných dôvodov nespokojnosti zákazníkov a z nich vyplývajúcich príčin odlivu spôsobených vnútornými faktormi podľa vyššie uvedeného zoznamu.

Druhým krokom je analýza vonkajšieho okolia firmy k čomu je možné využiť metódu SLEPTE (sociálne, legislatívne, ekonomické, politické, technologické a environmentálne faktory) spočívajúcu v kvalifikácii a kvantifikácii parametrov rozdelených do tematických skupín ako sociálne prostredie, legislatíva, ekonomický stav, politické prostredie, technologické reálie a životné prostredie. Cieľom tejto analýzy je zistenie či si firma môže dovoliť realizovať plánovanú zmenu.

Tretím krokom je aplikácia analýzy založenej na tzv. Porterovom modeli piatich konkurenčných síl, čo je metóda posúdenia externého konkurenčného prostredia firmy. Cieľom tejto analýzy je zistiť, či konkurenčné prostredie firmy umožní vykonať plánovanú zmenu. Taktiež môže viesť k identifikácii ekonomických rizík vyplývajúcich z nedostatočnosti výkonu

firmy v konkurenčnom prostredí, napr. nekonkurencieschopnosti poskytovaných služieb, teda v ich zaostávaní za konkurentmi.

Pre vyhodnotenie výsledkov získaných predchádzajúcimi čiastkovými analýzami sa používa záverečná zhrňujúca analýza, napr. SWOT. Tá slúži pre posúdenie silných a slabých stránok firmy a ich interakcie s príležitosťami a hrozbami ktoré firmu potenciálne čakajú.

Po vykonaní analýzy by mali byť dostupné všetky potrebné informácie pre naplánovanie samotnej zmeny. Pre systematický prístup je možné postupovať napr. podľa technokratického Lewinovho modelu. Ten je založený na posúdení síl – faktorov ovplyvňujúcich zmenu, či už zmenu podporujúcich alebo pôsobiacich proti nej.

V prvej fáze riadenia zmeny sa zostaví plán realizácie zmeny, čiže jej rozdelenie na jednotlivé čiastkové činnosti. Vo všeobecnosti môže byť zavedenie jednotlivých procesov vykonané paralelne, s občasnými vzájomnými závislosťami, plán implementácie by teda mal s týmto počítať.

V druhej fáze je vykonaná časová analýza pripraveného plánu zmeny. Je potrebné odhadnúť trvanie jednotlivých čiastkových činností a následne s prihliadnutím na ich vzájomné závislosti nájsť kritickú cestu takýmto grafom. K tomu je možné využiť napr. metódu PERT (angl. „Program Evaluation and Review Technique“, technika vyhodnotenia programu), ktorá počíta s neurčitosťou odhadu doby trvania jednorázových činností.

V tretej fáze sú identifikované a vyhodnotené riziká ohrozujúce vykonávanú zmenu. Vstupom pre analýzu rizík sú primárne ako slabé stránky a hrozby identifikované pri analýze SWOT, tak potom činnosti ležiace na kritickej ceste procesného grafu zmeny, najmä tie s vysokou smerodajnou odchýlkou doby trvania. Vhodnou formou reprezentácie je napr. mapa rizík ktorá rozdeľuje riziká podľa ich pravdepodobnosti a dopadu do postupných kategórií. Typicky sa volí rozdelenie oboch vstupov do troch či piatich stupňov a výstupného rizika do troch stupňov. Pre riziká spadajúce do dvoch najvyšších stupňov je nutné navrhnúť a implementovať nápravné opatrenia, pre riziká najnižšieho stupňa je možná retencia (podstúpenie) rizika.

4.2 Metódy technickej diagnostiky mobilných sietí

Termín diagnostika vychádza z lekárskych vied a znamená identifikáciu podstaty zdravotných problémov, ich klasifikáciu a vyhodnotenie. V technickej diagnostike ide analogicky o identifikáciu, klasifikáciu a vyhodnotenie symptómov indikujúcich odchýlku od normálneho stavu technického systému, kde výsledkom je diagnóza, na základe ktorej sa následne pokračuje opravou či optimalizáciou systému. Termín symptóm označuje indikátor, získaný pozorovaním či meraním nenormálneho stavu systému s určitou mierou istoty (pravdepodobnosti). Následne syndróm je množinou symptómov spoločne charakterizujúcich konkrétny nenormálny stav systému. Pri popise nenormálneho stavu hovoríme o poruchách (angl. „fault“) a zlyhaniach

(angl. „failure“). Zatiaľ čo porucha je stavom systému keď aspoň jeden z jeho komponentov či súčastí vykazuje degradované či nenormálne chovanie, zlyhanie je udalosť keď systém prestáva plniť aspoň jednu zo svojich funkcií. Po zlyhaní nasleduje v rámci technickej diagnostiky systematická analýza postihnutého systému, či jeho častí, vedúca k identifikácii prejavu zlyhania, jeho mechanizmu a príčiny (angl. „root cause“). Technickú diagnostiku teda môžeme definovať ako analýzu symptómov a syndrómov pre určenie podstaty porúch a zlyhaní technických systémov. [9]

Tradičný prístup k diagnostike, ale aj k výkonnostnému testovaniu mobilných sietí, podľa dokumentov 3GPP, je za pomoci výpočtu a porovnávania tzv. kľúčových výkonnostných indikátorov (KPI, angl. „Key Performance Indicator“), kde k ich získaniu môžu slúžiť, s rôznym stupňom výpovednej hodnoty, napr. dohľadový subsystém, drive testing, agenti na používateľských koncových zariadeniach či pasívne sondovanie rozhraní.

V prípade nutnosti ohodnotenia či optimalizácie siete sa ustanovia hladiny, ktoré musia hodnoty získaných indikátorov presiahnuť, aby sieť bola považovaná za dostatočne výkonnú. Tieto hladiny a aj skupiny indikátorov sú ale stanovované takmer až ľubovoľne, podľa preferencií konkrétneho operátora, dodávateľa technológie či firmy vykonávajúcej diagnostické a optimalizačné služby na konkrétnej sieti. To bohužiaľ vedie k získaniu a následnej práci s množinou čísel, ktorá je ťažko porovnateľná s prístupom a výsledkami inej autority.

Pri praktickej diagnostike mobilných sietí je veľmi dôležité vhodné zacielenie diagnostických zásahov. Tento problém je nutné riešiť individuálne, podľa podstaty diagnostického snaženia, napr. podľa predstavy zadávateľa o množine vyhodnocovaní parametrov. Typicky sa málo kedy diagnostikuje mobilná sieť ako celok, aj keď takýto postup je tiež možný, z veľkej časti preto, že správa mobilnej siete je organizačne delená do jednotiek, ktoré majú na starosti len konkrétne časti siete, či jej funkcie. Samozrejme pri takomto postupe s umelými administratívnymi prekážkami sa nie len znižuje efektivita diagnostiky, ale tiež je možné niektoré problémy, založené na vzájomnej interakcii jednotlivých subsystémov či funkcionality organizačných jednotiek zamaskovať natoľko, že ich odhalenie je prakticky nemožné.

Pri zameraní diagnostiky na konkrétnu časť mobilnej siete je ďalej vhodné obmedziť počet meracích miest, rozhraní a prvkov podľa konkrétnych požiadaviek. Toto umožňuje znížiť množstvo dát, ktoré je nutné spracovať, zjednodušuje technické riešenie diagnostiky a paradoxne to vedie k vyššej efektivite, pretože je možné vytvoriť popis presnejšie ilustrujúci konkrétny problém, obmedzenie služby či nedostatky prvku infraštruktúry. Rozsah diagnostických zásahov je nutné dobre naplánovať aj z organizačných dôvodov, napr. získanie povolenia k rozšíreniu pôsobnosti diagnostických činností pri ich výkone externým subjektom býva často, minimálne v krátkom čase, prakticky neriešiteľný administratívny problém.

Nasleduje popis jednotlivých metód získania surových dát, ich výhod a nevýhod v porovnaní s ostatnými metódami a potenciálom pre priame porovnávanie výsledkov pomocou nich získaných s výsledkami dosiahnutými pomocou využitia iných metód.

4.2.1 Dohľadový subsystém

Dohľadový subsystém ako integrálna súčasť ľubovoľnej komerčnej mobilnej siete je prvou voľbou pre diagnostiku siete, indikáciu a riešenie problémov. Jeho kvality a možnosti v tejto oblasti ale veľmi závisia na tom, čo implementoval jeho dodávateľ. Možnosť rozšíriteľnosti a doplnenia pôvodne nepodporovaných výkonnostných ukazovateľov je totiž väčšinou veľmi obmedzená.

Veľkou výhodou dohľadového subsystému oproti iným variantom je spravidla výrazne väčšia škála podporovaných výkonnostných indikátorov k podmienkam na rádiovom rozhraní. Údaje sú dostupné z pohľadu základňovej stanice, čo v podstate neumožňuje žiadna iná metóda. V prípade niektorých dodávateľov je tiež možné pracovať so štatistikami získanými z výsledkov meraní zasielaných mobilnými koncovými stanicami sieti pri rôznych príležitostiach. Takáto funkcia ale rozhodne nie je pravidlom u všetkých dodávateľov.

Funkčne dohľadový subsystém komunikuje so všetkými súčasťami mobilnej siete ktoré dohľaduje. Na získavanie údajov a štatistík o fungovaní týchto zariadení využíva ich vstavané meracie a reportovacie služby. Tieto dáta sú sprístupnené pomocou tzv. počítadiel (angl. counter). Z hodnôt počítadiel sa následne za použitia väčšinou len základných matematických operácií generujú ďalšie štatistiky ako rôzne súhrnné hodnoty či percentuálne vyjadrenia úspešností jednotlivých procedúr.

Z toho vyplývajú dve veľké nevýhody. Za prvé je nutné veľmi úzke prepojenie dohľadového susbsytému a dohľadovaného zariadenia, často nad rámec dostupných štandardov a teda sa jedná väčšinou o proprietárne riešenie, z čoho vyplýva potreba vytvorenia oboch častí jednou autoritou alebo veľké vynaložené úsilie v prípade dohľadového subsystému tretej strany. Existuje síce možnosť používať štandardné nástroje ako napríklad sprístupniť počítadlá pomocou protokolu SNMP (Simple Network Management Protocol, protokol pre vzdialený dohľad a správu sieťových zariadení), ale aj keď sa výrobca vydá touto cestou, stále nemusí sprístupniť popis svojej vetvy MIB (Message Information Base, stromová štruktúra definujúca systém informačných štruktúr o sieťovom zariadení pre použitie s protokolom SNMP) databázy, čo vec komplikuje skoro rovnako ako použitie vlastného komunikačného protokolu, tiež častý prípad. Druhým problémom je, že množina počítadiel nie je definovaná štandardom a závisí na implementácii výrobcu zariadenia. To znamená, že dostupné počítadlá sa líšia medzi zariadeniami rôznych výrobcov a tiež že počítadlá nie sú používateľsky definovateľné a teda rozšírenie v prípade potreby je veľmi zložité, vyžaduje spoluprácu s výrobcom zariadenia, tým pádom trvá dlho a je nákladné, vyžaduje tiež zmeny minimálne v programovom vybavení

zariadenia a teda následnú aktualizáciu, čo väčšinou znamená prerušenie služby. Bez ohľadu na ďalšie nevýhody je doba potrebná k sprístupneniu nových počítadiel a nutnosť aktualizácie programového vybavenia pre praktické použitie v diagnostickom procese diskvalifikačným faktorom. Takmer vždy, okrem dlhodobého monitorovania rozprestretého aspoň počas niekoľkých rokov a tým pádom zahŕňajúceho aj plánované aktualizácie, je teda nutné vychádzať len z údajov aktuálne zbieraných konkrétnym zariadením.

Na druhú stranu má táto situácia aj výhody. Prvou je väčšinou zanedbateľný až žiadny vplyv monitorovania na výkon a funkcie monitorovaného zariadenia. Získavanie hodnôt totiž rieši samotné zariadenie a toto je integrované do normálnej funkcionality zariadenia. Ďalšia veľká výhoda je, že je možné jednoducho získať aj parametre popisujúce interné chovanie zariadenia ako napr. reakcie na realizáciu procedúry vychádzajúce z vnútorného stavu zariadenia. Tieto údaje nie je rozumným spôsobom možné získať žiadnou inou dnes známou metódou.

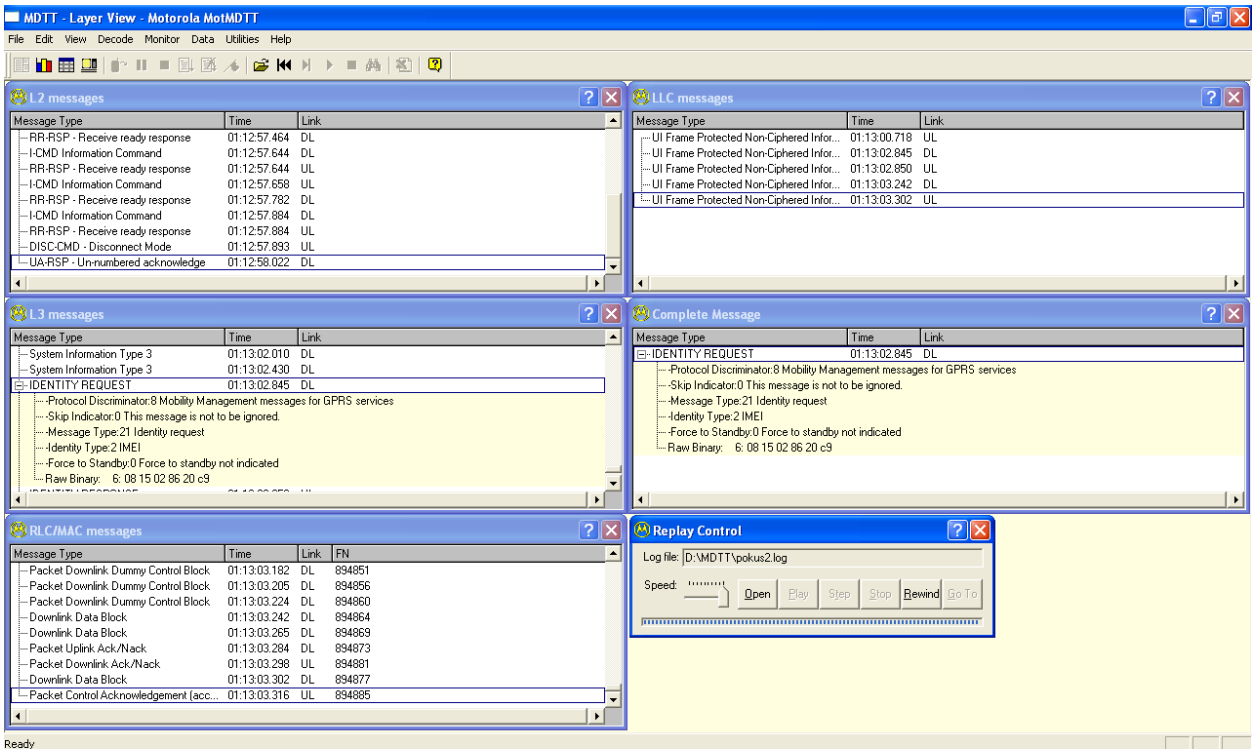
4.2.2 Drive testing

Metóda „drive testing“ je veľmi rozšíreným prístupom k výkonnostnému testovaniu mobilných sietí. Podstata tohto prístupu spočíva v realizácii aktívnych výkonnostných meraní v pohybe a rôznych geografických lokalitách pokrytých analyzovanou mobilnou sieťou. Merací systém je realizovaný programovateľným, špeciálne upraveným, terminálom mobilnej siete, ktorý v slučke realizuje rôzne procedúry ako pripájanie k mobilnej sieti a odpájanie, či realizuje telekomunikačné služby, napr. telefónny hovor, či definovanú dátovú službu.

V rámci testovania metódou „drive testing“ je možné sa zamerať na procedúry riadiacej roviny, ale tiež na služby v používateľskej rovine. Plán merania sa zostavuje dopredu a podľa skompilovaného zoznamu meraných služieb, procedúr a parametrov sa vybaví testovacie vozidlo meracími koncovými terminálmi v kombinácií s počítačom s programovým vybavením pre realizáciu meraní a záznam výsledkov. Veľmi dôležitou súčasťou je kontinuálny záznam polohy spolu s nameranými dátami. Pre túto metódu je projektom 3GPP vypracovaný zoznam kľúčových výkonnostných indikátorov aj s postupom merania, ako pre procedúry riadiacej roviny, tak pre realizáciu rôznych typov služieb nad paketovým dátovým spojením. Meranie je možné vykonávať pre rôzne rýchlosti pohybu koncových staníc, vrátane merania bez pohybu, keď sa dopravný prostriedok využíva len k presunom medzi meracími bodmi. Realizácia meraní s dynamickou rýchlosťou pohybu umožňuje, za cenu zvýšenia časovej a finančnej náročnosti, sledovať a analyzovať vyladenie operačných parametrov mobility účastníkov a vykonávať následnú optimalizáciu architektúry bunkového systému.

Častým prístupom k testovaniu metódou „drive testing“ je vykonávanie meraní na zákazku treťou stranou, väčšinou s porovnaním s mobilnými sieťami ostatných operátorov, keď sa počet koncových zariadení duplikuje podľa počtu alternatívnych mobilných sietí. Takto získané dáta umožňujú pre danú geografickú lokalitu porovnať performačné parametre mobilnej siete

a kvalitatívne parametre realizovaných služieb, medzi jednotlivými operátormi. Toto je možné považovať za najväčšiu výhodu tohto prístupu.



Obr. 2: Ukážka dekódovania správ rádiového rozhrania mobilnej siete nástrojom MDTT

Najväčšou nevýhodou tejto metódy je vysoká cena vyplývajúca z potreby vybavenia a prevádzky testovacieho vozidla s obsluhou, časovej náročnosti celého úkonu a nutnosti spracovávať dáta po skončení fázy merania s pomerne zložitou koreláciou. Ďalšou nevýhodou tejto metódy je praktické obmedzenie na konkrétne typy koncových zariadení, či už z pohľadu praktickej realizácie meraní väčšinou len na jednom type zariadenia, tak z pohľadu dostupnosti modelov testovacích koncových zariadení keď nie od každého je možné zaobstarať verziu upravenú pre realizáciu meraní metódou „drive testing“. Pomerne veľkou nevýhodou je aj praktická nereprodukovateľnosť výsledkov meraní, keď nezanedbateľný vplyv na aktuálne výsledky má charakteristika rádiového kanálu, ktorá sa spravidla v čase výrazne a pomerne rýchlo mení. Praktický dopad tohto problému je možné zmierniť zvýšeným počtom opakovaní celého merania, čo ale zase zvyšuje finančnú a časovú náročnosť.

Vo svojej podstate metóda „drive testing“ pristupuje k analyzovanej mobilnej sieti ako k čiernej skrinke keď je systém vybudený definovaným vstupom a následne analyzovaná jeho odozva. Z toho dôvodu je využitie metódy pre hľadanie podstaty problému malé, je možné získať len nepriame indície o poruchách bez hlbších poznatkov o dôvodoch.

Ukážka grafického používateľského prostredia drive testing nástroja MDTT (Motorola Drive Test Tool, nástroj pre meranie mobilných sietí metódou drive testing od firmy Motorola)

pre prostredie Microsoft Windows so zameraním na dekódovanie riadiacich správ na rádiovom rozhraní mobilnej siete je na Obr. 2.

4.2.3 Pasívne sondy rozhraní

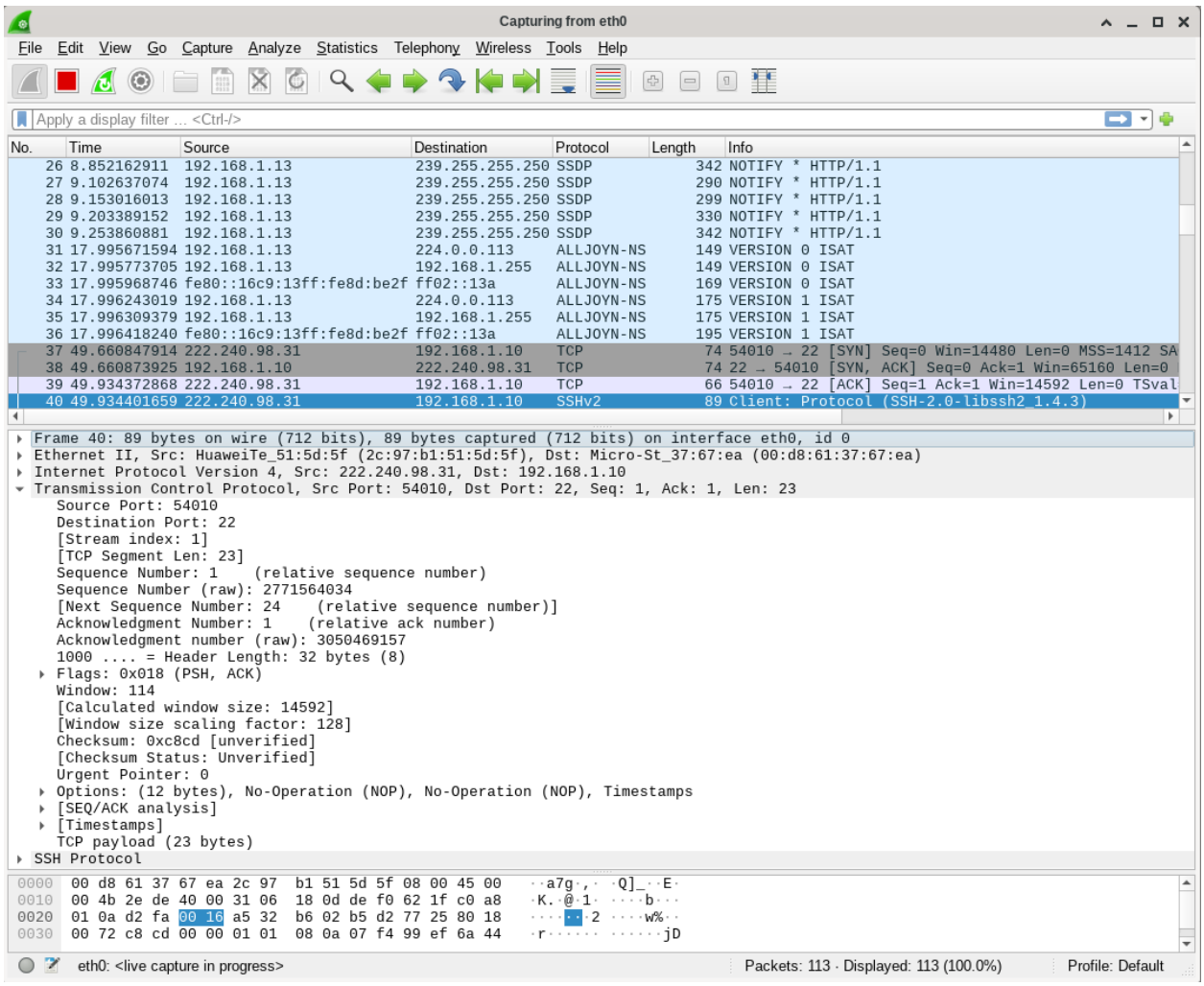
Využívanie pasívnych sond pre diagnostiku a predovšetkým monitorovanie mobilných sietí má historický obraz v telekomunikačnej technike, kde bolo použitie analyzátorov signalizácie na rôznych vrstvách rozšíreným prístupom, starším ako koncept plného dohľadového subsystému. Na druhú stranu je použitie pasívnych sond v dnešnej dobe výrazne inšpirované diagnostikou paketovo prepínaných dátových sietí, kde sa využívajú paketové zachytávače a analyzátory. Ako ich najvýznamnejšieho predstaviteľa je nutné spomenúť program Wireshark, ktorého používateľské rozhranie je zobrazené na Obr. 3.

Základom metódy je teda zachytávanie správ a dátových jednotiek, ich disekcia a zobrazenie v podobe zrozumiteľnej odbornej obsluhe. Doplňujúcimi funkciami je následná analýza, korelácia a štatistické spracovanie, umožňujúce kvantifikovať rôzne stavy, procedúry a chyby.

Podobným spôsobom pracujú komerčne dostupné pasívne sondy rozhraní mobilnej siete. Rozlišujú sa podľa podporovaných generácií mobilných sietí, kde niektoré sú zamerané len na konkrétnu generáciu, iné podporujú aj viacero generácii. V druhom prípade sú často zamerané na ekvivalentné rozhrania v architektúre mobilných sietí, napr. na rádiové rozhranie, či na rozhranie medzi účastníckym registrom a prvkom správy mobility. Zoznam podporovaných rozhraní u konkrétneho typu pasívnej sondy spravidla časom rastie z dôvodov konkurencie.

Ďalším dôležitým rozdeľujúcim kritériom je zameranie na používateľskú či riadiacu rovinu mobilných sietí. Historicky starším typom sú analyzátory zamerané čisto na signalizáciu. Tieto umožňujú pracovať s jednotlivými procedúrami riadiacej roviny, vyhodnocovať ich úspešnosť, či hľadať dôvody zlyhania. Ako také sú veľmi užitočným nástrojom pri inštalácii a oživovaní technológie mobilných sietí. Využijú sa ale aj neskôr, pri optimalizácii, pretože znížená úspešnosť realizácie procedúr riadiacej roviny na v podstate ľubovoľnom rozhraní či v prvku mobilnej siete má výrazne negatívny vplyv na performačné parametre mobilnej siete ako celku. Taktiež z globálneho hľadiska sa problémy riadiacej roviny diagnostikujú relatívne ľahko, pretože táto časť je dostatočne dobre popísaná v špecifikácii. Ďalej, vzhľadom na to, že najvýznamnejšou úlohou mobilných sietí, s predpokladom ešte väčšieho rastu do budúcnosti, je funkcia prístupovej siete k Internetu, je dôležitá analýza používateľskej roviny a teda zameranie pasívnych sond rozhraní na túto rovinu. Komunikácia v používateľskej rovine je z princípu podobná bežným dátovým sieťam založeným na protokole IP a teda sa tu využíva prenos signalizácie a používateľských dát jedným kanálom. Realizácia bežných služieb používateľmi teda netrpí len problémami riadiacej roviny, ale rovnako aj neúspechom signalizácie na z logického hľadiska vyššej vrstve, prenášanej v používateľskej rovine. Ďalší pohľad je

zameranie na prenášané používateľské dáta, kde podľa typu služby je možné kontrolovať parametre ovplyvňujúce kvalitu služby ako sú priepustnosť, latencia, kolísanie latencie v jednom smere, stratovosť a pod. Problémy s týmito parametrami sa neprejavujú neúspešnosťou služby, ale môžu narušiť kontinuitu služby či spôsobiť realizáciu služby s parametrami pre používateľa, či zo samotnej podstaty služby[8] neakceptovateľnými. Posledným variantom, naberajúcom na dôležitosti, je typ pasívnych sond podporujúcich analýzu ako riadiacej, tak používateľskej roviny, s rôznou, časom stúpajúcou, schopnosťou korelácie medzi nimi.



Obr. 3: Používateľské prostredie nástroja Wireshark

8 Príkladom by mohla byť realizácia služby prenosu hlasovej komunikácie pomocou paketových dát pri dobe RTT (angl. „Round Trip Time“, doba odpovede od protistrany) nad úrovňou umožňujúcou plynulú komunikáciu, stratovosť prekračujúcu korekčnú kapacitu kódovania pri rovnakej službe spôsobujúcu nezrozumiteľnosť reči, či primárne stratovosť či latencia v komunikácii spôsobujúca rozpad spojenia na transportnej vrstve v prípade využitia spoľahlivého prenosu či relačnej/aplikačnej vrstve v prípade nespoľahlivej služby.

Častým navrhovaným využitím pasívnych sond rozhraní mobilnej siete je v kontexte dlhodobého dohľadu nad sieťou s vyhodnocovaním prevádzkových štatistík tak, ako to umožňuje aj dohľadový subsystém. Toto použitie je často pretláčané marketingovými oddeleniami výrobcov pasívnych sond, ale z praktického hľadiska má len malý význam, nakoľko dohľadový subsystém už tieto funkcie zastáva a spravidla je súčasťou každej inštalácie. Naproti tomu využitie pri cielenej diagnostike mobilných sietí, kde sondy vynikajú nad relatívnou statickosťou dohľadového subsystému, je väčšou príležitosťou. S tým súvisí ďalšie kritérium rozdelenia pasívnych sond a to podľa spôsobu spracovania dát na sondy pracujúce v reálnom čase a sondy s odloženým spracovaním. Spôsob funkcie v reálnom čase je vhodný na dlhodobé monitorovanie, ale takmer nepoužiteľný pre diagnostické využitie. V prípade diagnostiky sa s výhodou uplatní záznam komunikačných dát s možnosťou neskôr, väčšinou iteratívne, analyzovať túto v čase zakonzervovanú vzorku. To umožňuje aj ľahšie porovnanie s dátami získanými z iných zdrojov a hľadanie príčin rozdielov. Nevýhodou, často prakticky neprekonateľnou z ekonomických dôvodov, je, najmä v prípade záznamu komunikácie v používateľskej rovine, potreba úložiska extrémnej kapacity a zápisovej rýchlosti, keďže priepustnosť rozhraní používateľskej roviny či podliehajúceho transportného jadra môže dosahovať rádovo stovky Gb/s a viac.

Veľkou výhodou použitia pasívnych sond rozhraní je možnosť dočasného monitorovania, v dnešnej dobe vzhľadom na schopnosti infraštruktúry transportného jadra ohľadom odbočenia a duplikovania sieťovej premávky, bez výpadku služby. Určitými nevýhodami je pomerne vysoká cena a množstvo byrokratických a administratívnych problémov súvisiacich s pripojením externých zariadení k existujúcej produkčnej infraštruktúre.

4.2.4 Agenti na používateľských koncových zariadeniach

Veľmi zaujímavou možnosťou, použiteľnou či už pre cielenú diagnostiku alebo dlhodobejšie monitorovanie používateľmi vnímaných parametrov, je využitie programového vybavenia nainštalovaného na koncových zariadeniach. Takíto agenti môžu buď pasívne monitorovať rádiové podmienky a parametre prenosu, alebo dokonca realizovať aktívne merania. Zozbierané dáta sa následne väčšinou centrálne analyzujú pre získanie štatistických indikátorov a podľa hĺbky a objemu zbieraných údajov je možné dokonca diagnostikovať konkrétne neštandardné situácie, ktoré zažívajú konkrétne koncové zariadenia. Výhodou je možnosť presnej lokalizácie meracieho bodu v čase a priestore s využitím satelitných pozičných systémov ako GPS (angl. „Global Positioning System“, satelitný systém pre určovanie polohy na zemeguli), Galileo (satelitný systém pre určovanie polohy na zemeguli), GLONASS (GLObal NAvigation Satellite System, satelitný systém pre určovanie polohy na zemeguli) či nový Čínsky satelitný navigačný systém BeiDou-3 (inštalácia zatiaľ poslednej tretej generácie bola dokončená v lete 2020). Väčšina koncových zariadení mobilných sietí má prijímač pre aspoň jeden z týchto systémov.

Úroveň monitorovania rádiového prostredia sa môže vyrovnať a dokonca predstihnúť možnosti dohľadového subsystému, zozbierané údaje sú ale lokálne pre konkrétne zariadenie a pri nízkom početnom nasadení väčšinou neponúkajú dostatočne detailné informácie pre vytvorenie máp pokrytia či ďalších všeobecných parametrov a indikátorov. Túto skutočnosť je možné zmierniť okrem zvýšenia počtu meracích staníc aj vyššou pohybovou aktivitou koncového zariadenia či agregáciou výsledkov z dlhšieho časového úseku.

Možnosť realizovať aktívne meranie dáva tejto metóde predpoklady vyrovnať sa drive testom. Agent môže buď na pokyn obsluhy, alebo plne autonómne vykonávať v podstate všetky testy, ktorými disponujú dostupné DTT (angl. „Drive Test Tool“, nástroj na meranie parametrov mobilných sietí metódou drive testing). Ďalšou výhodou je možnosť nasadenia na rozličné modely koncových zariadení a z toho vyplývajúce posúdenie správania sa konkrétneho typu zariadenia v danej sieti s prípadným následným diagnostickým a optimalizačným zásahom.

Táto metóda je v súčasnosti veľmi zriedkavo využívaná. Do budúcnosti je možné predpokladať výrazné rozšírenie kvôli relatívne malému množstvu, navyše pomerne jednoducho odstrániteľných, nevýhod a veľkej výhody v jednoduchosti a v porovnaní s ostatnými metódami takmer zanedbateľnej cene. Pokiaľ by operátor mohol nasadiť túto technológiu na významné množstvo používateľských koncových zariadení svojich zákazníkov, získal by lacný a celkom presný spôsob získavania informácií o zákazníkmi vnímaných parametroch siete, navyše výsostne z lokalít, v ktorých sa používatelia reálne pohybujú.

4.3 Podporné metódy

Okrem zastrešujúcich metód pre analýzu rizík a diagnostiku mobilných sietí sa používajú aj ďalšie čiastkové nástroje. Významnú úlohu pri analýze systémov komplexnosti mobilných sietí hrá popisná štatistika, ktorá umožňuje charakterizovať analyzovanú veličinu. Druhým podobným nástrojom sú tzv. kľúčové výkonnostné indikátory (KPI, angl. „Key Performance Indicator“), čo je otvorená množina meraných a častejšie dopočítavaných kompozitných veličín, ilustrujúcich stav mobilnej siete ako technického systému a jej pripravenosť na plnenie požadovaných primárnych či doplnkových funkcií.

4.3.1 Štatistické nástroje

Aplikácia štatistických metód umožňuje vyčíslenie sekundárnych výkonnostných indikátorov, zameraných na odhad podstaty porúch a nežiaducich či negatívne sa prejavujúcich dejov v analyzovanom systéme. Klasický diagnostický prístup k mobilným sieťam ale štatistické metódy v podstate nevyužíva. Pri vyčíslovaní výkonnostných indikátorov, sa v priemyselnej praxi pri diagnostike mobilných sietí využíva často len priemer ako vyjadrenie strednej hodnoty. To je samozrejme veľmi dôležité, nakoľko to umožňuje korekciu vplyvu náhodných javov, ale

pri využití ďalších štatistických nástrojov, napr. vyčíslovania momentov vyšších rádov, je možné získať užitočné informácie, ktoré inak zostávajú skryté. Tieto nové informácie majú často výrazný dopad na pokračovanie diagnostického procesu, okrem indikácie stavu ukazujú aj na jeho možné príčiny, čím zrýchľujú diagnostické práce a skracujú čas výpadku systému v prípade poruchy. Teoretický základ k nižšie uvedeným štatistickým veličinám je možná nájsť napr. v [16].

Pre príklad zoberme hodnotu doby odpovede vzdialeného systému v používateľskej rovine mobilnej siete. Máme množinu realizácií meraní tohto parametru ktorú berieme ako štatistický súbor. Klasický prístup je výpočet aritmetického priemeru $\hat{x}$ podľa vzorca:

$$\hat{x}=\frac{\sum_{j=1}^{n} x_j}{n} \tag{1}$$

kde n je veľkosť štatistického súboru a x_j je iterátor nad štatistickým súborom. Takto získaná stredná hodnota ako bolo spomínané obmedzuje vplyv náhody. Vypočítaný aritmetický priemer sa teda berie ako reprezentatívna hodnota strednej doby odpovede vzdialeného systému, na základe ktorej sa usudzuje o stave systému. Pokiaľ hodnota prekročí nejakú určenú hranicu, stav sa vyhlási za nevyhovujúci a nasleduje ďalšia diagnostika tohto stavu z iných zdrojov. Takto získaný parameter teda spĺňa detekčnú potrebu, ale k skutočnej diagnostike je jeho použitie málo významné. Ak teda stredná hodnota doby odpovede indikuje nevyhovujúci stav, môžeme pokračovať výpočtom ďalších parametrov.

Doplňme teda aritmetický priemer výpočtom rozptylu podľa vzorca:

$$\sigma^2=\frac{1}{n}\sum_{j=1}^{n}\left(x_j-\hat{x}\right)^2 \quad , \tag{2}$$

kde n je znovu veľkosť štatistického súboru, x_j je iterátor nad štatistickým súborom a $\hat{x}$ je aritmetický priemer vypočítaný podľa vzorca (1). Rozptyl nám pridá o dobe odpovede vzdialeného systému doplňujúcu informáciu. Presné hranice závisia od prípadu, ale vo všeobecnosti pokiaľ je pomer rozptylu k strednej hodnote malý, doba odpovede je stabilná, čo ukazuje na systémový problém v transportnom jadre mobilnej siete. Potenciálne dôvody sú napríklad využitie linky s vysokou latenciou alebo zlej konfigurácie smerovania, kde sa využíva alternatívna linka s väčším počtom skokov k cieľu. Na druhú stranu ak je pomer rozptylu k strednej hodnote veľký, doba odpovede sa často mení, čo indikuje zahltenie prvku či linky po transportnej trase. Tu môžeme doplniť využitie minima štatistického súboru. Ak by toto minimum spadalo dostatočne hlboko pod spomínanú detekčnú hranicu, problém bude čisto ohľadom zahltenia prvku či linky, ak je blízke tejto hranici, jedná sa o akúsi kombináciu oboch problémov.

Ďalším vhodným indikátorom je výpočet šikmosti štatistického súboru podľa vzorca:

$$\gamma_1 = \frac{\sum_{j=1}^{n} \left(x_j - \hat{x} \right)^3}{n \cdot \sigma^3} \quad , \tag{3}$$

kde n je veľkosť štatistického súboru, x_j je iterátor nad štatistickým súborom, $\hat{x}$ je aritmetický priemer vypočítaný podľa vzorca (1) a σ je smerodajná odchýlka vypočítaná podľa vzorca:

$$\sigma = \sqrt{\sigma^2} \tag{4}$$

dosadením do vzorca (2). Získaný parameter šikmosti popisuje asymetriu rozdelenia štatistického súboru, hodnota blízka nule znamená symetrické rozdelenie, kladná hodnota šikmosti indikuje výskyt odľahlých realizácií smerom k maximu, záporná zase smerom k minimu. Vyššie kladné hodnoty v prípade vyhodnocovania doby odpovede vzdialeného systému teda indikujú výskyt občasných realizácií s pridanou väčšou latenciou, čo je prípad napr. zariadenia po ceste nespĺňajúceho podmienky na systém pracujúci v reálnom čase[9].

Podobne je možné takýto postup aplikovať na ďalšie výkonnostné indikátory, na prvý pohľad sa ponúkajú doby obsluhy požiadaviek v riadiacej rovine, kde je podstata takmer identická. Prakticky ale podobne ide hodnotiť akýkoľvek výkonnostný indikátor po spracovaní potrebnej teórie a praktickom overení. Ďalej je možné skúmať využitie ďalších, pokročilejších štatistických nástrojov ako testy príslušnosti k rozdeleniu, množstvo parametrov vykazuje binomické či ešte viac modálne rozdelenia, tam je možné určovať podstatu zo vzájomných posunov módov a pod.

4.3.2 Kľúčové výkonnostné indikátory

Vo všeobecnosti môžeme pri telekomunikačných systémoch hovoriť o výkonnostných indikátoroch, viažúcich sa k procesom, procedúram či jednotlivým parametrom. Napr. publikácia [18] definuje množinu všeobecných výkonnostných indikátorov, ktoré sú platné pre posúdenie parametrov v podstate ľubovoľného telekomunikačného systému, ako popisuje Tab. 1. Takto je možné popisovať všeobecný komunikačný či proste obsluhový systém. Pre diagnostiku a výkonnostné testovanie mobilných sietí sa používa sada tzv. kľúčových výkonnostných indikátorov, množinou parametrov definovanou organizáciou 3GPP, ohľadom ktorých je všeobecný konsenzus, že požadovaný popis siete a chovania služieb dokážu zabezpečiť.

9 Systém pracujúci v reálnom čase (angl. „real-time system“) garantuje obsluhu požiadavku najneskôr v definovanom čase.

Tab. 1: Všeobecné výkonnostné indikátory technických systémov

Parameter	**Popis**	**Matematické vyjadrenie**
Presnosť	stupeň zhody medzi nameranou a požadovanou hodnotou	$P\left(\left\|d_i - d_{m,i}\right\| \le \varepsilon_d\right) \ge \gamma_d$ (5)
Spoľahlivosť	schopnosť systému realizovať obsluhu požiadavku bez prerušenia v priebehu časového intervalu	$P\left(\left\|v_t - v_{m,t}\right\| \le \varepsilon_s\right) \ge \gamma_s, t \in \langle 0, T \rangle$ (6)
Dostupnosť	schopnosť systému iniciovať obsluhu požiadavku	$P\left(\left\|q_{m,i} - q_i\right\| \le \varepsilon_d\right) \ge \gamma_d$ (7)
Kontinuita	schopnosť systému plniť svoje funkcie bez neplánovaného výpadku v priebehu obsluhy požiadavku či v dobe časového intervalu	$P\left(\left\|r_t - r_{m,t}\right\| \le \varepsilon_k\right) \ge \gamma_k, t \in \langle 0, T \rangle$ (8)
Integrita	schopnosť systému včasne a bezchybne informovať o nemožnosti obslúženia konkrétneho požiadavku	$P\left(\left\|s_i - s_{m,i}\right\| \le \varepsilon_i\right) \ge \gamma_i$ (9)
Bezpečnosť	schopnosť systému neohroziť svoje okolie v prípade poruchy	$P\left(\left\|W_i - W_{m,i}\right\| \le \varepsilon_b\right) \ge \gamma_b$ (10)

Organizácia 3GPP venovala kľúčovým výkonnostným indikátorom množstvo dokumentov, napr. [22] pre všeobecné KPI z riadiacej roviny, ďalej [23] a [24] zamerané na rádiovú prístupovú sieť 3,9G a 4G; KPI pre 2G a 3G sú zase v [25]. Kľúčovými výkonnostnými indikátormi v IMS (angl. „IP Multimedia Subsystem“) sa zaoberá [26], KPI pre jadro siete 3,9G a 4G rieši [27].

Okrem KPI definovaných organizáciou 3GPP je množstvo doplnkových, s ktorými prichádzajú operátori mobilných sietí a tiež výrobcovia zariadení infraštruktúry mobilných sietí. Problematika KPI mobilných sietí presahuje rámec tejto práce, dobrým úvodom do problematiky je napríklad [28] a príklady konkrétnych KPI, ako pre riadiacu, tak používateľskú rovinu, a postupu ich získania sú uvedené v prílohe č. 3.

4.4 Zhrnutie kapitoly

Táto kapitola bola venovaná metódam posúdenia bezpečnosti a výkonnosti mobilných sietí. Jednotlivé metódy boli analyzované, charakterizované a posúdené z hľadiska využiteľnosti pri práci s mobilnými sieťami.

Prvou skupinou boli metódy analýzy rizík a posúdenia bezpečnosti z oblasti obecného inžinierstva rizík. Jednalo sa o analýzu spôsobov a dopadov porúch FMEA, analýzu stromu udalostí ETA, analýzu stromu porúch FTA, analýzu príčin a následkov CCA, univerzálnu maticu rizikovej analýzy UMRA, analýzu ľudskej spoľahlivosti HRA, kontrolného zoznamu, diagramu rybacej kosti a metód posúdenia ekonomických rizík 7S, SLEPTE, Porterovho modelu a analýzy SWOT. Pre použitie v oblasti mobilných sietí sa obecne javí ako veľmi výhodná metódy UMRA pre prehľadovú analýzu, či metóda FMEA pre identifikáciu možných nepreviazaných porúch a

ich dopadov. Ostatné metódy sú využiteľné skôr pre konkrétne činnosti: ETA pre modelovanie procedúr a ich možných koncových stavov, kontrolný zoznam pre činnosti vykonávané personálom s nižšou odbornosťou, CCA ako dokumentácia porúch od príčin k dôsledkom, FTA alebo diagram rybacej kosti pre hľadanie príčinných súvislostí vedúcich k nežiadúcim stavom, HRA pre posúdenie vplyvu ľudského faktora pri neautomatizovaných činnostiach a analýzy ekonomických rizík pri realizácii zmien a posúdenie možných negatívnych dopadov.

Ďalšou skupinou metód sú metódy technickej diagnostiky vychádzajúce z praxe prevádzky mobilných sietí. V tejto skupine ide o monitorovanie s využitím dohľadového subsystému mobilnej siete, meranie parametrov mobilnej siete s využitím metódy drive-testing alebo pasívnych sond na rozhraniach mobilnej siete, či meracích agentov na používateľských koncových zariadeniach. Tieto metódy je možné využiť samostatne, prípadne ich kombinovať, čo často výrazne skracuje čas potrebný pre nájdenie porúch. Pri výbere vhodnej metódy či ich kombinácie je potrebné zvážiť konkrétnu situácie a analyzovaný problém. Dohľadový subsystém je prítomný v každej sieti a jeho využitie je ľahké a netvorí ďalšie náklady, množina monitorovaných parametrov ale nebýva veľká a najmä ich nie je možné priamo porovnávať s hodnotami získanými z dohľadových systémov od iných dodávateľov a niekedy ani s hodnotami získanými inými metódami. Pasívne sondy rozhraní monitorujú komunikáciu v pevnej časti siete, takže podávajú len nepriame dôkazy k situácii na rádiovom rozhraní a preto že pracujú s obrovskými objemami dát, sú drahé a niekedy náročné na čas. Na druhú stanu umožňujú veľmi presné výsledky a zachytenie chýb ktoré neobjavia žiadne iné metódy, prípadne dokonca lokalizáciu chyby aj keď jednotlivé časti fungujú ako čierne skrinky. Drive-testing je najtradičnejšia metóda ktorá rozoznáva, že problémy mobilných sietí vyplývajú najmä z ich rádiového rozhrania. Meria parametre služieb z pohľadu používateľa a dokáže veľmi presne monitorovať procesy na rádiovom kanále. Na druhú stranu merania sú do istej miery syntetické, vyžadujú veľa času a vysoko odborný personál, čím sú extrémne drahé a ich schopnosť odhaľovať poruchy inde ako na rádiovom rozhraní je malá. Nakoniec agenti na používateľských termináloch sú lacné a umožňujú merať parametre služieb ako ich vníma používateľ. Z pohľadu siete sa jedná o najmenej intruzívnu metódu, avšak z pohľadu používateľa a ochrany jeho súkromia môžu byť výrazne intruzívne. V praxi sa ukazuje ako dobré riešenie kombinácia metódy pasívnych sond rozhraní s aspoň jednou ďalšou metódou.

Uvedené zastrešujúce metódy sú doplnené čiastkovými, konkrétne sa využíva popisná štatistika pre charakteristiku veličín a teda chovania meraného systému a ďalej z praxe analýzy mobilných sietí vychádza používanie kľúčových výkonnostných indikátorov ako kvantitatívnych ukazovateľov spoľahlivosti, výkonu a prevádzkových parametrov poskytovaných služieb.

Všetky metódy analýzy rizík, posudzovania bezpečnosti, výkonnosti a spoľahlivosti mobilných sietí vyžadujú znalosti štruktúry, vlastností prvkov, komunikačných ciest a požadovaného správania častí mobilnej siete, či ich vzájomnej interakcie. Tento potrebný model si vyžaduje aplikáciu systémového prístupu k problematike.

5 Systémový prístup k problematike mobilných sietí

Systémový prístup je metodológia myslenia a konania vo vzťahu k rôznym entitám, definujúca aké podstatné skutočnosti by mali byť zohľadnené v činnostiach s entitou a ako by tie činnosti mali byť realizované [12].

V rámci aplikácie systémového prístupu k riešenému problému je potrebná diskusia možností využitia mobilných sietí pre zabezpečenie funkcií kritickej infraštruktúry štátu, výroby a služieb. Je potrebné analyzovať technické a organizačné požiadavky na komunikačné mobilné siete vyplývajúce z potreby zabezpečenia uvedených funkcií. Z konštrukcie komunikačného systému potom vychádzajú zraniteľnosti – predispozície k určitým konkrétnym hrozbám.

Z pohľadu interakcie mobilných bunkových sietí s inými kritickými infraštruktúrami a celkovo širším okolím do ktorého sú zasadené vyvstáva špeciálne potreba vyššej pripravenosti v prípade narušenia iných kritických infraštruktúr či mimoriadnej situácie / núdzového stavu. Z toho vyplýva zvýšenie personálneho zabezpečenia, venovaných zdrojov na rozvoj a udržanie robustnosti mobilných sietí, revízia a zlepšenie núdzových plánov podľa špecifík konkrétnej situácie a pri dlhšom trvaní aj teoretický rozvoj častí realizácie kritických služieb a robustnosti. Tiež sa v takom prípade ustupuje od nákladových optimalizácií a kladie vyšší dôraz na redundanciu, statické či exkluzívne vyhradenie prostriedkov ale siaha sa aj k prostriedkom provizórneho navýšenia prepojovacej kapacity siete, napr. zahustenia rádiovej prístupovej siete mobilnými základňovými stanicami.

5.1 Štruktúra a okolie mobilnej siete

Problematiku mobilných bunkových sietí v roli kritickej komunikačnej infraštruktúry a analýzu rizík pre takúto sústavu je pre efektívne zvládnutie nutné rozdeliť na jednotlivé časti a venovať sa im zvlášť, následne zohľadniť vzťahy medzi týmito časťami a vzťahy celej sústavy k okoliu, aby sa dodržali zásady systémového prístupu k problematike. Prvou časťou je mobilná sieť, najmä jej architektúra, prvky a funkcie. Druhou časťou je problematika kritickej infraštruktúry, požiadavky na systémy pracujúce v takejto roli a to špeciálne na komunikačnú kritickú infraštruktúru. Treťou časťou je legislatívny rámec ohľadom kritickej infraštruktúry a normatívny rámec ohľadom robustnosti mobilných bunkových sietí a zachovania telekomunikačných funkcii v krízových situáciách.

5.1.1 Architektúra mobilnej bunkovej siete

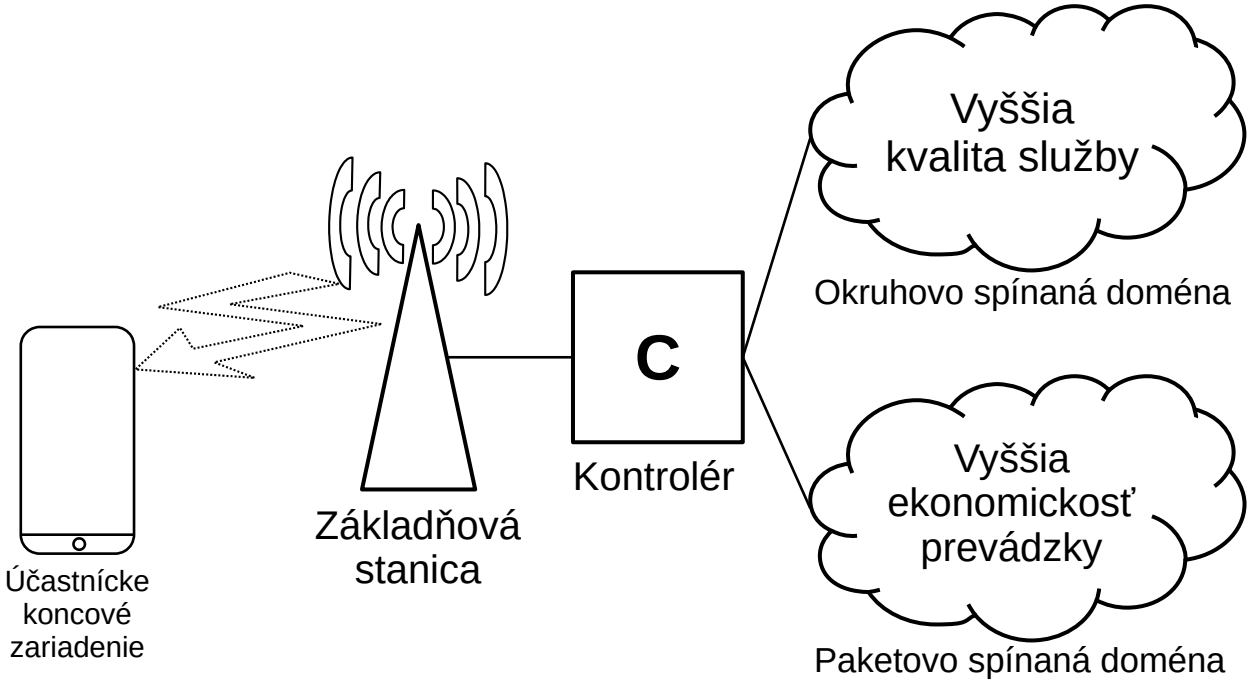
Kompletná architektúra mobilnej siete, najmä v prípade posledných generácií či multigeneračných inštalácií, je značne zložitá, pozostávajúca z množstva prvkov vzájomne prepojených niekoľkými desiatkami rozhraní. Koncepčne sa ale môžeme pozrieť na aktuálne

používané mobilné siete druhej, tretej, štvrtej a piatej generácie, a nájsť spoločné rysy. Schéma všeobecnej architektúry mobilnej siete vypracovaná týmto postupom je zobrazená na Obr. 5. Z tejto schémy bude vychádzať ďalší popis.

Obr. 4: Základňová stanica mobilnej siete s anténami na stožiari

V mobilnej sieti je vždy prítomná základňová stanica (angl. „base station“), zobrazená na Obr. 4, ktorá realizuje sieťovú časť rádiového spoja s účastníckym koncovým zariadením. Z jedného fyzického miesta vysielať niekoľko buniek, typicky v rôznych geografických smeroch či inak určených pre pokrytie odlišného územia (napr. nastavením azimutu antény), prípadne

pracujúcich na iných frekvenčných kanáloch, pričom každá obsluhovaná vlastnou základňovou stanicou. Viaceré smery od stožiara ale môžu byť súčasťou jednej bunky, najmä v odľahlých oblastiach (prípad inštalácie na Obr. 4), bez znalosti architektúry siete to nie je pohľadom možné odlíšiť. Následne je v sieti riadiaci prvok základňových staníc (angl. „base station controller“), ktorý je od 4G (mobilná sieť štvrtej generácie) integrovaný so základňovou stanicou, naopak v predchádzajúcich generáciách mohol riadiť aj viac ako jednu základňovú stanicu. Tieto dva funkčné prvky tvoria rádiovú prístupovú sieť.



Obr. 5: Vysokoúrovňová architektúra mobilnej bunkovej siete

Rádiová prístupová sieť sa následne napája na okruhovo spínané jadro alebo paketovo spínané jadro, dnes typicky oboje. Pôvodne sa používalo len okruhové spínanie a uvedená architektúra vyplýva z toho, že podpora paketových prenosov bola do mobilnej siete integrovaná doplnením takmer nezávislého paketovo spínaného jadra a zdieľaním rádiovej prístupovej siete s časovým oddelením pre oba typy prenosu. Okruhovo spínaná a paketovo spínaná doména sa z pohľadu prevádzkovaných služieb od seba líšia najmä poskytovanými parametrami kvality služieb a možnosťou zdieľania infraštruktúry. Zatiaľ čo prenosy pomocou okruhového spínania ponúkajú službu s nízkou latenciou a jej kolísaním za cenu vyhradenia prostriedkov pre konkrétneho používateľa počas celej doby realizácie služby, prepínanie paketov umožňuje efektívnejšie zdieľanie prostriedkov medzi jednotlivými používateľmi a službami, čo umožňuje znížiť prevádzkové náklady, následne cenu telekomunikačnej služby a tiež lepšie škáluje s počtom používateľov a umožňuje uspokojiť požiadavky na vyššiu špičkovú či okamžitú požadovanú prenosovú rýchlosť v prípade nízkeho vyťaženia ostatnými používateľmi.

Z hľadiska diagnostiky veľmi dôležitou časťou mobilnej siete, ktorá ale na Obr. 5 nie je zobrazená, je transportné jadro (angl. „transport core“) alebo tiež nosná sieť (angl. „backhaul“). Úlohou tohto subsystému je prenos komunikácie medzi jednotlivými prvkami mobilnej siete zahŕňajúcej ako signalizáciu, tak, čo do dátového objemu významnejšie, tunelované používateľské dáta. Funkčnosť transportného jadra sa priamo prejavuje na spoľahlivosti a výkone mobilnej siete, keď v prípade problémov v tejto oblasti dochádza k výraznej degradácii všetkých kvalitatívnych parametrov. Historicky boli pre realizáciu nosnej siete používané najmä dva varianty líšiace sa podobne ako okruhovo a paketovo spínané jadro a vychádzajúce z filozofie týchto dvoch systémov. Pre potreby realizácie okruhovo komutovaných služieb a teda historicky starší je prenosový systém založený na časovom delení do slotov využívajúci technológiu E1/T1 (systém časovo deleného multiplexovaného prenosu dát využívajúci časové sloty), ponúkajúci nízku latenciu s prakticky nulovým kolísaním a konštantnú prenosovú rýchlosť. Tento systém umožňuje aj prenos paketovo prepínaných služieb, ale za cenu zníženia efektivity a zvýšenia zložitosti kvôli nutnosti využitia prenosu vo viacerých časových slotoch. Pre realizáciu paketovo komutovaných služieb je vhodnejšie použitie tohto typu prenosu, zväčša založenom na rodine technológií Ethernet. Prenos okruhovo spínaných dát je v tomto prípade možný tiež, pre zabezpečenie kvality služby sa využíva naddimenzovanie prenosového systému. Treťou možnosťou je využitie systému založeného na prepínaní buniek, napr. ATM (angl. „Asynchronous Transfer Mode“, technológia telekomunikácie založenej na prepínaní buniek), ktorá teoreticky umožňuje lepšiu podporu kombinovaného prenosu okruhovo a paketovo komutovaných služieb, v praxi je ale efektívnejšie, najmä z ekonomického hľadiska, využitie rozumne naddimenzovaného paketovo spínaného transportného jadra.

5.1.2 Interakcia mobilnej siete s inými kritickými infraštruktúrami

Vzhľadom na význam kritickej infraštruktúry pre zabezpečenie základných funkcií je pochopiteľné, že jednotlivé kritické infraštruktúry využívajú služby iných kritických infraštruktúr, navzájom sa ovplyvňujú a závisia na sebe. Na druhú stranu obmedzenie akejkoľvek kritickej infraštruktúry už z definície kritickej infraštruktúry vlastne vždy negatívne ovplyvní ostatné kritické infraštruktúry. Také uvažovanie nevedie k záverom na základe ktorých by sa dalo užitočne konať, preto je potrebné pri analýze závislostí rozlišovať primárnu závislosť pri ktorej sa priamo využívajú služby inej kritickej infraštruktúry a sekundárnu závislosť kde obmedzenie služby v špeciálnych prípadoch a stredne až dlhodobom pôsobení má negatívny vplyv na dostupné zdroje (čo je pri kritickej infraštruktúre vždy).

V prípade mobilných bunkových sietí ako špeciálneho prípadu telekomunikačnej kritickej infraštruktúry, existuje primárna závislosť na dodávkach elektrickej energie a teda táto kritická infraštruktúra priamo využíva služby elektrickej rozvodnej siete a celého odvetvia elektroenergetiky.

5.1.3 Interakcia mobilnej siete s technickým prostredím

Technické prostredie mobilnej bunkovej siete okrem služieb poskytovaných inými kritickými infraštruktúrami a interakcie s nimi je definované najmä podpornou infraštruktúrou pre budovanie rádiovej siete a rádiovým komunikačným kanálom. Podporná infraštruktúra rádiovej siete je súbor prírodných geografických čŕt, človekom vybudovaných stavieb a technických podporných zariadení pre polohovanie a prevádzku základňových staníc mobilnej siete. Rádiový komunikačný kanál využíva šírenie elektromagnetického žiarenia vo verejnom prenosovom prostredí. Na komunikáciu sa používajú vyhradené licencované kmitočtové pásma, napriek tomu môže dochádzať k rušeniu a tým zníženiu odstupu signálu od šumu SNR, udávaný v $[dB]$, definovaný ako pomer výkonu signálu k výkonu šumu, čo je základný parameter určujúci spoľahlivosť komunikácie a dostupnú šírku pásma. Rádiová komunikácia tiež trpí tým, že je zachytiteľná aj inými subjektami ako sú účastníci komunikácie[10], čo je nutné technicky kompenzovať, typicky kryptograficky pomocou šifrovania prenášaných dát.

Vlastnosťou rádiového komunikačného kanálu je útlm, označovaný A – pokles intenzity signálu so vzdialenosťou prenosu médiom, udávaný v dB/m. Ten má dve zložky, prirodzenú vychádzajúcu zo znižovania hustoty energetického toku S šírením guľovou plochou:

$$S = \frac{P}{4\pi r^2}; \left[\frac{W}{m^2}\right], \tag{11}$$

kde P je vysielací výkon a r je vzdialenosť od zdroja vysielania; a náhodnú vychádzajúcu z vlastností prostredia ako je prítomnosť mechanických prekážok či vplyvu aktuálneho počasia. Šum je prítomnosť iných signálov, ktoré z hľadiska analyzovaného systému nie sú užitočné.

5.1.4 Interakcia mobilnej siete s používateľmi

Nové generácie mobilných sietí sa prispôsobujú potrebám a problémom používateľov a spoločnosti ako celku, je ale možné sledovať aj opačný smer vplyvu. Mobilné siete výrazným spôsobom zmenili to, ako používatelia pristupujú ku konzumácii obsahu a medziľudskej komunikácií tým, že poskytujú stále dostupné, mobilné pripojenie. Na základe týchto možností tiež vznikajú nové služby, napr. celá kategória tzv. „cloudových“ služieb, kde dáta sú uložené centrálne a používateľské koncové zariadenie je len terminálom poskytujúcim prístup k týmto dátam a k službám založeným na ich vzdialenom spracovaní.

S narastajúcou priepustnosťou rádiovej prístupovej siete mobilných sietí sa tiež zvýrazňuje tendencia používateľov využívať mobilné pripojenie tak, ako by používali pevné pripojenie v domácnosti. Typický používateľ chce prístup k svojej palete služieb bez ohľadu na to, ako je

10 Myslí sa čisto komunikácia rádiovým kanálom v konfigurácii bod-bod, teda medzi základňovou stanicou a mobilným používateľským koncovým zariadením; nejedná sa o komunikáciu medzi dvoma účastníkmi

technicky zabezpečená sieťová konektivita. A moderné mobilné siete tieto požiadavky podporujú.

Podľa štúdie [29] je technologický rozdiel medzi 3G a 4G sieťami tak výrazný, že používateľ v 4G sieti prenesie 10x až 100x viac dát ako v 3G, ak nie je obmedzovaný limitmi FUP (angl. „Fair Usage Policy“, politika férového využívania služby) a pokrytie je dostatočne kontinuálne aby nedochádzalo k prepojeniu do staršej generácie mobilnej siete. Mobilná sieť s rádiovou prístupovou sieťou LTE (angl. „Long Term Evolution of the UMTS“, rádiová prístopová sieť 3,9G) poskytuje lepšiu službu ako verejné WiFi (angl. „Wireless Fidelity“, bezdrôtové počítačové siete) siete, používatelia viac dáta odosielajú, využívajú mobilné pripojenie ako jediné či primárne, pokrývajúce všetky ich telekomunikačné potreby [29]. V [29] sa tiež spomína nárast využívania streamovaného videa na úkor konzumácie informačne identického písaného textu, ale iná štúdia, [30], explicitne tvrdí, že 78% používateľov stále preferuje písaný text pretože je podľa nich rýchlejší a praktickejší na konzumáciu, či im nevyhovuje agresívna reklama, ktorá videu často predchádza. Pomerne znepokojivým zistením, publikovaným v [30], je, že až 51% používateľov uvádza využívanie sociálnych sietí pre získavanie informácií, až pre 12% sa dokonca jedná o hlavný zdroj. Ďalšou dôležitou informáciou je, že 53% používateľov, ako hlavné zariadenie pre prístup k informačným zdrojom, využíva mobilný terminál.

Vo výročnej správe Českého telekomunikačného úradu za rok 2020 [31] sú, okrem iného, uvedené aj informácie k stavu telekomunikačného trhu, ktorého sú mobilné siete dôležitou súčasťou. Podľa tejto analýzy v roku 2020 existovalo u všetkých operátorov v Českej republike 9,7 milióna aktívnych SIM (angl. „subscriber identity module“, modul identity účastníka) kariet, ktoré mobilnými sieťami v priemere preniesli mesačne približne 3,15GB dát. Uvádzané sú aj hodnoty z predchádzajúcich rokov a tak je možné vidieť, že u oboch sledovaných parametrov sa jedná o exponenciálny rast. Zároveň je v [31] konštatovaný pokles ceny za prenos jednotky dátového objemu a to na asi 0,5 Kč/MB. Z ďalších uvádzaných informácií je tiež zrejmé, že mobilné telekomunikácie rástli v roku 2020 v Českej republike viac ako ostatné sledované typy telekomunikácie spolu, čo potvrdzuje status mobilných sietí ako kritickej komunikačnej infraštruktúry.

Je možné pozorovať, že všadeprítomné mobilné siete, rastúce schopnosti používateľských koncových zariadení využívaných ako terminály v mobilných sieťach a meniace sa zvyky používateľov vytvárajú navzájom sa podporujúci ekosystém so stupňujúcou sa, kladnou, spätnou väzbou.

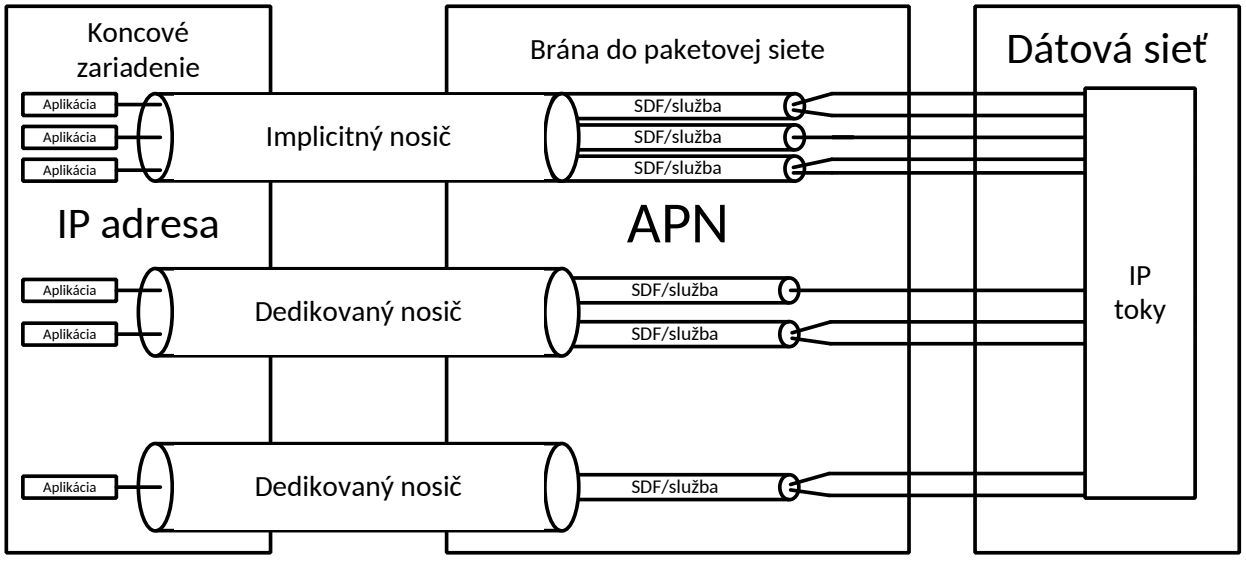
5.2 Vnútorná štruktúra a vzťah medzi prvkami

Mobilná sieť je komplexným systémom skladajúcim sa z mnohých prvkov a majúcim zložitú štruktúru vzťahov medzi týmito prvkami. Funkcionalita mobilnej siete je založená na takejto

štruktúre a pre spoľahlivé fungovanie na ňu kladie vysoké nároky. Spoľahlivosť realizácie telekomunikačných služieb založených na prepínaní dátových jednotiek je založená na alokácii zdrojov a prioritizácii prednosti pri prenose aj zahadzovaní pri preťažení. Tieto činnosti sa dohromady nazývajú zabezpečením kvality služby.

5.2.1 Zabezpečenie kvality služby

Podpora zabezpečenia kvality služby (QoS, angl. „Quality of Service“) v mobilných sieťach je potrebná z dôvodu limitovanej priepustnosti rádiového rozhrania mobilnej siete, najmä v dobe zvýšenej záťaže, a nutnosti realizovať súčasný prenos mnohých typov služieb, využívaných viacerými používateľmi. V prípade realizácie okruhovo spínanej hovorovej služby je zabezpečenie kvality služby implicitné pomocou dopredného vyhradenia prostriedkov naprieč celou komunikačnou infraštruktúrou. Zložitejšia je situácia v prípade využívania paketovo prepínaných dátových služieb, ktoré sú v prípade mobilných sietí generácie 3,9G a vyššej využívané aj pre hovorovú službu, tzv. VoLTE (angl. „Voice over LTE“, prenos hovorových cez paketovo prepínanú doménu). Architektúra podpory kvality služby pre paketové dátové prenosy v mobilnej sieti ilustrujúca vzájomné vzťahy je zobrazená na Obr. 6.



Obr. 6: Zabezpečenie kvality služby paketových dátových prenosov v mobilnej sieti

Pre logické vyčlenenie paketovej dátovej komunikácie jedného koncového zariadenia sa využíva v mobilných sieťach koncept paketového dátového kontextu, čo je asociácia sieťovej adresy koncového terminálu a prístupového bodu k vonkajšej paketovej sieti APN (angl. „Access Point Name“, názov prístupového bodu). V prípade, že jedno koncové zariadenie je pripojené k viacerým paketovo orientovaným sieťam, existuje pre neho teda niekoľko paketových dátových kontextov. V druhej a tretej generácii mobilných sietí sa paketový dátový kontext

nazýva PDP (angl. „Packet Data Protocol“, protokol pre prenos paketovo orientovaných dát v systémoch založenych na GPRS[11]) kontextom, v systémoch SAE (angl. „System Architecture Evolution“, evolúcia architektúry jadra siete v mobilných sieťach 3,9G a 4G) zase PDN (angl. „Packet Data Network“, identifikátor paketového dátového spoja v mobilných sieťach 3,9G a 4G) spojom.

Následne pre logické rozlíšenie kategórií realizovaných služieb v rámci jedného paketového dátového kontextu je používaný koncept tzv. nosičov (angl. „bearer“). Nosič je virtuálne spojenie definované množinou parametrov podľa ktorých infraštruktúra mobilnej siete s tokmi prenášanými týmto nosičom zaobchádza. Vždy je vytvorený jeden implicitný nosič (angl. „default bearer“), ktorý poskytuje transport typu best-effort, bez garantovania prenosovej rýchlosti. Ak je určitý tok či toky nutné prioritizovať s určitými parametrami, je preň vytvorený vyhradený nosič (angl. „dedicated bearer“). Nosiče v rámci jedného paketového dátového kontextu zdieľajú jednu adresu sieťovej vrstvy (IP adresu), priradenú pri vytváraní implicitného nosiča. Vyhradené nosiče môžu byť s garantovanou (tzv. GBR – angl. „Guaranteed Bit Rate“, systém zabezpečenia kvality služby s vyhradením pásma pre konkrétnu službu či skupinu služieb) alebo negarantovanou prenosovou rýchlosťou (tzv. Non-GBR). Ďalšími parametrami sú priorita používaná pri spracovaní v plánovači paketov (angl. „packet scheduler“), horná hranica oneskorenia paketov a paketová chybovosť, definujúca maximálnu hodnotu pomeru počtu neprijatých paketov k odoslaným. Ďalším, veľmi dôležitým, parametrom nosiča je ARP (angl. „Allocation and Retention Priority“, priorita prideľovania a uchovania), ktorý definuje na úrovni riadiacej roviny prioritu vytvorenia nosiča na úkor iných či jeho zrušenia v prípade vyčerpania kapacity. Jedná sa len o binárnu funkciu existencie konkrétneho nosiča v konkurencii ostatných nosičov, ktorá nemá, na rozdiel od predchádzajúcich parametrov, vplyv na prenos jednotlivých paketov.

V rámci jedného nosiča je možné prenášať niekoľko služieb, definovaných pomocou SDF (angl. „Service Data Flow“, vzor dátovej služby), kde každá služba môže pozostávať z jedného alebo viacerých používateľských tokov[12]. Agregácia jednotlivých používateľských tokov (v používateľskej rovine definovaných napr. pomocou tzv. 5-tuple, t.j. kombinácie zdrojovej a cieľovej IP adresy, protokolu a zdrojového a cieľového portu transportnej vrstvy) do SDF je vykonávaná na základe TFT (angl. „Traffic Flow Template“, vzor premávkového toku).

Zabezpečenie kvality služby v transportovanej používateľskej rovine je ďalšia záležitosť. Túto problematiku je ale tiež potrebné riešiť, pretože podpora kvality služby musí byť realizovaná E2E (angl. „End to End“, po celej dĺžke trasy), pretože degradáciu na čiastkovom

11 General Packet Radio Service, prenos paketovo orientovaných dát rádiovým rozhraním mobilnej siete GSM.

12 Služby často využívajú paralelne niekoľko spojení (tokov), typicky napr. oddelené riadiace a dátové spojenie v prípade služby prenosu súborov FTP (angl. „File Transfer Protocol“, protokol pre prenos súborov) či oddelené spojenie pre signalizáciu a hlasové dáta v prípade komunikačnej služby v architektúre SIP (angl. „Session Initiation Procotol“, signalizačný protokol pre VoIP službu) – angl. „Voice over IP“, prenos hovorov cez IP sieť.

úseku nie je možné korigovať inde. Je preto vhodné medzi používateľským koncovým zariadením a druhou komunikujúcou stranou niekde v Internete realizovať zabezpečenie kvality služby pomocou metód známych z dátových sietí.

5.2.2 Historický vývoj mobilných sietí

Najvýznamnejšou technickou prerekvizitou pre mobilnú telekomunikáciu je realizácia dátového prenosu rádiovými vlnami. Po prvých demonštráciách Heinricha Hertza (1888), Nikoly Tesly (1893) a Alexandra Stepanoviča Popova (1895) sa ako prvá komerčne úspešná technológia komunikačného prenosu rádiovými vlnami ukázal bezdrôtový telegraf Guglielma Marchese Marconiho (1897). Systém ale využíval kódovanie Morseovou abecedou a nejednalo sa o prenos hlasu.

Systémy pre mobilnú telefóniu sa začali objavovať v 20-tych rokoch 20. storočia, napr. medzi silovými a policajnými zložkami USA (angl. „United States of America“, Spojené štáty americké) a tiež pre použitie v námornej komunikácii. Neskôr malo kladný vplyv začatie využívania frekvenčnej modulácie, čo sa prejavilo najmä v rádiokomunikačných systémoch počas druhej svetovej vojny. Následne sa vojenská technológia začala využívať pre poskytovanie mobilnej telefónnej služby vo väčších amerických mestách, ale s veľmi limitovanou kapacitou.

Prvá generácia mobilných sietí, od 70-tych rokov 20. storočia, využívala analógový prenos a najväčšie zlepšenie bolo zavedenie bunkového systému. To umožňovalo pokrytie ľubovoľne veľkého územia s využitím obmedzeného frekvenčného pásma a z toho vyplývajúcu možnosť kapacitného škálovania siete. Patria sem systémy ako AMPS (angl. „Advanced Mobile phone system“, mobilná sieť prvej generácie) v USA a Japonsku, severoeurópsky NMT (angl. „Nordic Mobile Telephone“, mobilná sieť prvej generácie) či britský TACS (angl. „Total Access Communication System“, variant AMPS). Veľmi aktívne bolo Nemecko s jeho troma subgeneráciami analógových systémov A-Netz (1958), B-Netz (1972) a C-Netz (1985).

Najväčšie zlepšenie druhej generácie bolo zavedenie digitálneho prenosu a časového či kódového multiplexovania a s ním spojený výrazný nárast prenosovej kapacity mobilných sietí. Ďalším zlepšením je zavedenie voliteľného šifrovania signalizácie a hovorových dát, z používateľského a obchodného hľadiska zase zavedenie veľkej škály doplnkových služieb a najmä služba prenosu krátkych správ v GSM (angl. „Global System for Mobile communications“, mobilná sieť druhej generácie). Sieť GSM tiež umožňovala okruhovo spínaný prenos dát, tzv. CSD (angl. „Circuit Switched Data“, prenos, spravidla paketovo orientovaných, dát ponad okruhovo spínaný spoj v rádiovej prístupovej siete v mobilných sieťach), ktorý sa v dobe zavedenia vyrovnal možnostiam CSD prenosov v pevných telefónnych sieťach, no neskôr začal rýchlo zaostávať. Okrem GSM v Európe boli vyvinuté a nasadzované ďalšie technológie pre siete druhej generácie, využívané najmä v USA, napr. vylepšené verzie systému AMPS: IS-

54B (digitálny prenos hlasu, analógová signalizácia) a neskôr plne digitálny systém IS-136, či tiež IS-95 CDMA (technológia Qualcomm).

Ďalej štandardizačný proces prešiel pod organizáciu 3GPP a tak začala práca na tretej generácii mobilných sietí. Nové myšlienky ale mali vplyv aj na druhú generáciu, kde niektoré technológie a postupy boli spätne portované pre využitie v sieťach druhej generácie, najmä pre zlepšenie návratnosti vybudovanej infraštruktúry a urýchlenie dostupnosti týchto technológií pre používateľov – zákazníkov. Najdôležitejšou takouto technológiou je podpora paketového prenosu dát GPRS, ktorá rozširuje GSM sieť o paketové jadro a upravuje rádiovú prístupovú sieť pre umožnenie takýchto prenosov. Upravená sieť sa označuje za sieť 2,5G. Neskôr bola tiež podobne implementovaná technológia EDGE (angl. „Enhanced Data rates for Global Evolution“, zlepšenie technológie GPRS, zvyšujúce prenosové rýchlosti využitím výkonnejších modulačných a kódových schém), ktorá zaviedla nové kódové schémy a tým priniesla zvýšenie priepustnosti prenosu paketových dát po rádiovom rozhraní. Umožnenie prenosu paketovo spínaných dát výrazne zlepšilo dostupnosť a praktickú využiteľnosť mobilných dátových služieb, nakoľko kvôli lepšiemu zdieľaniu zdrojov viedlo k zníženiu cien, keď zákazník platí len za prenesené dáta bez ohľadu na dobu pripojenia. To umožňuje používateľom byť stále dostupnými aj v rámci dátových služieb a teda napr. priebežnú mobilnú prácu s e-mailom.

Nevýhodou GSM bolo to, že sa jednalo o európsky štandard a napriek veľkému rozšíreniu existovali a boli nasadzované konkurenčné nekompatibilné riešenia a tak stále nebolo možné využívať skutočný globálny roaming. Toto sa snaží riešiť tretia generácia mobilných sietí, kde v podstatnej väčšine krajín sveta bola nasadená technológia UMTS (angl. „Universal Mobile Telecommunications System“, mobilná sieť tretej generácie). Okrem tohto štandardu sa prakticky používa len konkurenčný CDMA2000 (evolúcia IS-95 CDMA) a aj to len obmedzene v USA a Južnej Kórei, kde v oboch krajinách sú dostupné aj siete založené na technológii UMTS. Tretia generácia mobilných sietí sa okrem zlepšenia možností paketového prenosu dát zvýšením prenosových rýchlostí a znížením latencie, špeciálne v nadväzujúcich technológiách rodiny HSPA (angl. „High Speed Packet Access“, systém pre zvýšenie prenosovej rýchlosti paketových dát v sieti UMTS), začala viac na paketovo prepínanú doménu spoliehať. Plánovalo sa všeobecné nasadenie videotelefónnej služby využívajúcej paketovo prepínaný prenos dát a riadenej subsystémom IMS. Táto služba sa ale nikdy nedokázala komerčne presadiť, kvôli nedostatočnému vybudovaniu sietí tretej generácie v dobe nasadzovania, nekompetitívnemu naceneniu a predovšetkým kvôli nízkej praktickej pridanej hodnote pre používateľov v porovnaní s klasickou telefónnou službou.

Štvrtá generácia mobilných sietí kompletne vypúšťa okruhovo spínanú doménu. To znamená, že telefónne hovory musia byť riešené buď dočasným prepnutím do paralelne vybudovanej siete 2G (mobilná sieť druhej generácie) či 3G (mobilná sieť tretej generácie), technológia sa označuje CSFB (angl. „Circuit Switched Fall-Back“, technológia využitia k sieti štvrtej generácie paralelne prevádzkovanej siete druhej či tretej generácie pre prenos okruhovo

spínaných telefónnych hovorov počas doby ich realizácie) [17], keď sieť štvrtej generácia slúži len pre dátové prenosy, alebo neskôr s využitím technológie VoLTE, ktorá je aplikáciou VoIP (angl. „Voice over Internet Protocol“, prenos hlasových hovorov cez paketovo orientované dátové siete) do mobilných sietí. Využívanie len paketovo prepínaného prenosu umožňuje zjednodušenie architektúry mobilnej siete a tiež lepšie zdieľanie prostriedkov a teda zvýšenie praktickej kapacity mobilnej siete, najmä z hľadiska počtu paralelne obsluhovaných koncových zariadení. To je veľmi dôležité kvôli veľkému nárastu počtu koncových zariadení, najmä kvôli IoT (angl. „Internet of Things“, komunikačný systém pre fyzické zariadenia) a M2M (angl. „Machine to Machine“, komunikácia dvoch fyzických zariadení), keď mobilnú sieť využívajú okrem ľudí aj stroje a zariadenia, a to vo veľkom rozsahu, ale väčšinou s malými objemami dátových prenosov.

Piata generácia mobilných sietí má riešiť problémy ako zvýšenie maximálnej priepustnosti komunikácie, zníženie spotreby elektrickej energie mobilných terminálov a tým zvýšenie výdrže na batériu, zlepšenie pokrytia či ďalšie zníženie latencie prístupovej siete. Najväčšou výzvou ale bude riešenie problému škálovateľnosti, nakoľko sa predpokladá rapídny rast počtu pripojených koncových zariadení, najmä z oblasti M2M, pričom v podstate všetky budú neustále vyžadovať vysokú dostupnosť služby.

V súčastnosti sú väčšinou jedným operátorom paralelne prevádzkované prepojené siete druhej, tretej a štvrtej generácie súčasne, s testovacími, geograficky a zákaznícky obmedzenými, nasadeniami sietí piatej generácie. To umožňuje znížiť náklady na budovanie infraštruktúry, najmä využitím kombinovaných základňových staníc, ale tiež pokrývaním novou technológiou prednostne lukratívnych územných častí, keď v ostatných dočasne postačuje aj len technológia staršej generácie. Z pohľadu diagnostiky ale takéto riešenie v podstate exponenciálne zvyšuje náročnosť a tiež sťažuje testovanie konfiguračných zásahov mierených na zlepšenie parametrov siete pred finálnym nasadením.

Prechod medzi generáciami mobilných sietí bol vždy z dôvodu riešenia konkrétneho problému. Medzi prvou a druhou generáciou sa jednalo o nahradenie analógového systému prenosu digitálnym, čo prinieslo výrazné navýšenie kapacity siete. Druhá generácia mobilných sietí, najmä systém GSM stále výborne spĺňa požiadavky na hovorovú službu. Jej schopnosti poskytovať dátovú službu boli zlepšené zavedením podpory prenosu paketových dát GPRS, ktorý ale reálne podporuje len základné dátové služby a nespĺňa požiadavky na moderné služby. Zabezpečenie prenosových parametrov mobilnej siete bolo riešené generáciou treťou, ktorá mierne zvýšila priepustnosť, ale najmä znížila latenciu prístupovej siete. Generácia štvrtá ďalej znížila latenciu, ale jej najväčším prínosom bolo masívne navýšenie priepustnosti rádiovej prístupovej siete. Vývoj pochopiteľne nebol skokový a preto sa preto existujú prechodové technológie a zlepšenia, keď sa myšlienky novej generácie v obmedzenej forme aplikujú na generáciu predchádzajúcu. To umožňuje zlepšenie poskytovanej služby skôr, s menšími nákladmi a dočasné odloženie vybudovania mobilnej siete novej generácie.

5.3 Služby v mobilných sieťach

Mobilné siete pochopiteľne neexistujú samoúčelne, ale preto, aby používateľom poskytovali telekomunikačné služby. Operátor mobilnej siete za poskytované telekomunikačných služieb získava finančné prostriedky a vzhľadom na konkurenčné prostredie je potrebné, aby zabezpečoval dostačujúcu kvalitu služby a parametre siete pre zachovanie spokojnosti zákazníkov. V priebehu času vzniklo množstvo rôznych telekomunikačných služieb poskytovaných nad mobilnými sieťami, majúcich často veľmi rôzne požiadavky na kvalitu služby.

5.3.1 Služby okruhovo spínanej domény

Historicky najstaršia transportná a prepínacia časť mobilných sietí, okruhovo spínaná doména, ktorá je základom mobilných sietí druhej, v určitej forme prvej a v podstate aj tretej generácie, podporuje väčšinu klasických telekomunikačných služieb, v prvom rade službu hovorovú. Pre prenos hovorových dát je tento typ spojovania optimálny, nakoľko umožňuje výborné zabezpečenie kvalitatívnych požiadaviek služby ako nízke oneskorenie a kolísanie oneskorenia. Vzhľadom na používané kódovanie pre prenos dát je následne dimenzovaná kapacita prepojovaných jednotiek a prepojovacích uzlov a hovorová služba tak má v okruhovo spínanej doméne podpornú infraštruktúru s dostatočnými a veľmi stabilnými parametrami.

Oproti klasickým pevným telekomunikačným sieťam musí ústredňa mobilnej siete naviac riešiť problematiku mobility používateľa a je teda viac logicky prepojená s prístupovou sieťou, kde hovor od konkrétneho koncového zariadenia môže prísť z v podstate ľubovoľnej časti prístupovej siete a takisto môže byť počas doby trvania prepájaný podľa pohybu používateľa a jeho koncovej stanice.

Nad okruhovo spínanou doménou je možné okrem telefónneho hovoru realizovať aj dátové prenosy pomocou technológie CSD, podobnej vytáčanému dátovému spojeniu z pevných telefónnych sietí, ponúkajúcej dátové služby s nízkou latenciou a konštantným dátovým tokom.

Okrem hovorovej služby a ďalších základných služieb podporuje okruhovo spínaná doména aj širokú škálu služieb doplnkových, najmä ohľadom rôznych variantov indikácie čísla volajúceho účastníka, multiplexovania hovorov (konferenčný hovor, pridržanie hovoru) či presmerovania prichádzajúceho hovoru za rôznych okolností.

5.3.2 Paketovo orientované OTT služby

Najvýznamnejšou paketovo orientovanou OTT (angl. „Over The Top", transportovaná služba) službou je prístup k sieti Internet, aj keď v mobilných sieťach je pomerne časté sprostredkovanie pripojenia účastníckeho koncového zariadenia do iných, privátnych, dátových sietí, označované

ako VPN (angl. „Virtual Private Network“, tunelované pripojenie používateľského koncového zariadenia k lokálnej dátovej sieti) služba. Bez ohľadu na typ cieľovej dátovej siete je spravidla realizovaný prenos používateľských dát pomocou protokolu IP, i keď použitie iného prenosového protokolu je taktiež možné.

Protokol IP následne umožňuje transport všetkých bežných služieb protokolovej sady TCP/IP (protokolová sada používaná v sieti Internet) ako v iných dátových sieťach. Veľmi častou službou je prenos webového obsahu pomocou protokolu HTTP (angl. „HyperText Transfer Protocol“, protocol pre prenos hypertextových dokumentov a ďalších dát), ďalej e-mail a tiež rôzne služby prenosu súborov. Z pohľadu diagnostiky sa analýza používateľskej roviny mobilných sietí teda nelíši od analýzy prenosov v akejkoľvek inej dátovej sieti.

Dôležitou skupinou, ktorej význam v čase narastá, sú multimediálne prenosy. Multimediálne prenosy po paketovo orientovaných sieťach je možné rozdeliť do dvoch kategórií, na prenosy v reálnom čase a na streamované multimediálne prenosy. Tieto skupiny sa líšia najmä požiadavkami kvality služby, ale obe kladú na sieť relatívne veľké nároky, typicky do značnej miery protichodné, pretože pre prenosy v reálnom čase je potrebná nízka latencia a teda doba odozvy systému, zatiaľ čo pre streamované multimediálne služby je to vysoká priepustnosť. Pri praktickej realizácii sa tieto dve požiadavky ukazujú ako protichodné, čo komplikuje návrh jednotlivých zariadení a tiež infraštruktúry ako celku.

Ďalším typom paketovo orientovaných služieb sú služby realizované pomocou multicastových prenosov, špeciálne služby zamerané na distribúciu dátového obsahu ale tiež prenosy masového streamovania multimediálneho obsahu, napr. televízneho vysielania.

Dôležitou, s predpokladaným rastom významu do budúcnosti, dátovou OTT službou je zabezpečenie komunikácie typu IoT či M2M, kde komunikujúce strany priamo nezahŕňajú ľudského účastníka. Systémy priemyselnej automatizácie využívajúce mobilné siete ako prístupové komunikačné siete sú bežnou praxou. Výsledkom je napríklad senzorický systém, ktorý počíta s možnosťou využiť pre prenos dát konektivitu mobilnej siete ako záložnú možnosť v prípade výpadku hlavnej transportnej technológie.

5.3.3 Služby integrované do siete

Už od svojho počiatku boli mobilné bunkové siete vystavované problému, že pre zabezpečenie špeciálnych požiadaviek a funkcií potrebovali integrovať ďalšie služby. Zrejme najznámejšou službou, ktorá bola integrovaná do mobilných sietí, je služba posielania krátkych správ SMS (angl. „Short Message Service“, služba prenosu krátkych správ). Riadiace prvky mobilnej siete, signalizácia na jednotlivých rozhraniach a zodpovedajúce procedúry sú vytvorené či rozšírené tak, aby sieť podporovala natívne túto novú, integrovanú službu. Služby integrované do siete sú napr. k paketovo orientovaným OTT službám kontrastné tým, že k ich realizácii sa využíva

signalizácia v riadiacej rovine mobilných sietí a sú zabezpečované prvkami mobilnej infraštruktúry namiesto aplikačných serverov v sieti Internet.

Príkladom modernej služby integrovanej do mobilnej siete je sieťou riadená priama komunikácia medzi používateľskými koncovými stanicami na základe geografickej blízkosti.

Ďalšou službou či skôr sadou služieb vyžadujúcou špecializované procedúry riadiacej roviny a podporu v zariadeniach sieťovej infraštruktúry je zabezpečenie požiadaviek na kvalitu služby pre podporu komunikačných potrieb kritickej infraštruktúry štátu a priemyslu. V minulosti boli pre takéto účely budované vyhradené siete, napr. na základe technológie TETRA (angl. „Terrestrial Trunked Radio“, systém pre obojsmernú mobilnú komunikáciu s automatickým prepínaním komunikačných kanálov), čo je ale finančne pomerne náročné. Pre prenos napr. správ nižších stupňov utajenia je použitie bežných sietí, ak umožňujú zabezpečiť požiadavky na kvalitu týchto kritických služieb, akceptovateľné a vítané.

5.4 Obecné zraniteľnosti mobilnej bunkovej siete

Architektúra a technická realizácia mobilnej bunkovej siete vychádzajú z inžinierskej praxe, výskumu problematiky a zo skúseností. Z toho dôvodu je možné nájsť spoločné znaky s inými štruktúrami podobnej zložitosti, účelov a vlastností. S takýmito štruktúrami ale mobilná sieť rovnako zdieľa zraniteľnosti vyplývajúce z návrhu a realizácie.

5.4.1 Zraniteľnosti zálohovaných systémov

Zálohovanie systémov je metóda pre zvyšovanie spoľahlivosti systémov pomocou zámerne zabudovaných nadbytočných prvkov. Problematika zálohovania v technických systémoch presahuje rámec tohto dokumentu, poznámky k zálohovaným systémom a spoľahlivosti sú uvedené v prílohe č. 2.

Zraniteľnosti zálohovaných systémov vychádzajú z nedostatočnosti zvoleného spôsobu zálohovania vzhľadom k použitiu daného technického systému. V zásade môžeme identifikovať tri druhy zraniteľností. Prvým druhom zraniteľnosti je tzv. *centrálny bod zlyhania* (angl. „Single Point of Failure“, SPoF), čo je vynechanie konkrétnej časti systému zo zálohy, napriek tomu, že iné časti systému sú zálohované. V prípade SPoF je v rámci určitej procedúry či procesu niektorý z využívaných prvkov bez zálohy a v prípade jeho zlyhania teda dôjde k obmedzeniu danej funkcie systému ako celku. Dôvody k tejto zraniteľnosti bývajú ako v nedostatočnosti analýzy v dobe návrhu, tak ekonomické, keď sa zo zálohy vynechá príliš drahá komponenta. Alternatívne môže byť SPoF prvok mimo oblasť vplyvu a zodpovednosti architekta či implementátora a byť využívaný ako externá služba.

Druhým druhom zraniteľnosti je hrozba tzv. *kaskádového zlyhania* (angl. „cascading failure“), ktorá vzniká v prípade že redundancia prvkov sa nevyužíva výlučne pre zálohu, ale aj

pre rozkladanie záťaže. V takomto prípade je obsluha požiadaviek rozkladaná na batériu funkčne rovnakých prvkov vhodným algoritmom a v prípade výpadku kritického množstva prvkov je pomerná časť záťaže priveľká pre niektorý ďalší prvok, ten je preťažený a zlyháva, čo navyšuje záťaž ďalších prvkov a vedie k reťazi zlyhaní. Dôvodom tohto stavu je chyba v analýze požiadaviek a z toho plynúca nevhodná kombinácia zálohy a rozkladania záťaže. Riešením je naopak striktné oddeľovanie zálohovania systémov ako metódy pre zvyšovanie spoľahlivosti a rozdeľovania záťaže ako metódy hromadnej obsluhy.

Tretím druhom zraniteľnosti zálohovaných systémov, ktorý sa v príslušnej literatúre uvádza len zriedkavo, je hrozba tzv. *synchronizovaného zlyhania*, čo je stav, keď viaceré prvky zálohy sú zraniteľné voči konkrétnej hrozbe. Typicky sa jedná o jednu z mnohých hrozieb a k tejto zraniteľnosti dochádza v prípade nedostatočnej analýzy požiadaviek na systém a jeho spoľahlivosť. Záloha je konfigurovaná tak, že zvažované hrozby sú ňou pokryté, ale systém je ohrozovaný aj ďalšou hrozbou proti ktorej je záloha neúčinná. V prípade mobilných sietí je to napríklad prípad, keď viaceré základňové stanice v jednej oblasti využívajú rovnaké frekvenčné pásmo. To umožňuje výber základňovej stanice s najvyšším odstupom signálu od šumu a tiež chráni pred výpadkom niektorej zo základňových staníc. Takto zálohovaný systém je ale zraniteľný voči lokálnemu rušeniu na komunikačnej frekvencii, ktoré postihuje komunikačné kanály voči všetkým takýmto základňovým staniciam. Obranou voči tejto zraniteľnosti je svedomitá analýza rizík a následný návrh zálohy tak, aby prvky netrpeli spoločnými hrozbami.

5.4.2 Zraniteľnosti rozľahlých systémov

Bežná mobilná sieť z podstaty veci typicky pokrýva celú krajinu v ktorej je prevádzkovaná, inak by nemohla byť zabezpečená mobilita používateľov, čo je najväčšia výhoda mobilnej siete. Sieť teda pokrýva pomerne rozľahlé územie a musí s týmto faktom pracovať. Aj v prípade komunikácie geograficky blízkych účastníkov typicky komunikácia, minimálne signalizácia, prechádza jadrom siete, ktoré môže byť vzdialené.

Ďalej prípadná cezhraničná mobilita používateľa je zabezpečená tzv. medzinárodným roamingom[13]. V tomto prípade tečie signalizácia a dáta realizovaných služieb sieťami oboch operátorov, ako domáceho v krajine pôvodu, tak hostiteľského v krajine pohybu používateľa. Toto sa deje z viacerých dôvodov, napr. pre účtovanie prenosov ale aj kvôli zabezpečeniu národných legislatívnych požiadaviek na riadenie prístupu a zaznamenávanie metadát o komunikácii.

Mobilná sieť teda je rozľahlým systémom a pri jej návrhu a optimalizácii treba počítať s problémami z toho vyplývajúcich. V prípade komunikácie vnútri siete je potrebné zabezpečiť takú prenosovú trasu dát, aby nedochádzalo k zbytočnému navyšovaniu transportného

13 Presah rádiového vysielania z jednej krajiny do druhej je problematický z hľadiska zákonnosti a aj keď sa v prihraničných oblastiach občas vyskytuje, jedná sa v podstate o nežiadúci stav.

oneskorenia. Toto je nutné riešiť ako na úrovni transportného jadra siete *hľadaním optimálnej trasy*, tak na úrovni používateľskej roviny, *výberom blízkeho prvku* pri rozkladaní záťaže. V prípade duplikácie prvkov totiž tie bývajú umiestnené v rôznych lokalitách okrem iného z dôvodu riešenia problému rozľahlosti[14]. V prípade komunikácie účastníkov v rozdielnych sieťach sa k týmto problémom pridáva potreba *vhodného geografického umiestnenia a logického zapojenia prvkov využívaných pre signalizáciu medzi sieťami*. Tá vyvstáva bez ohľadu na to, ktorá sieť je pre účastníkov komunikácie domácou a ktorá hostiteľskou, či na geografickú oblasť prevádzky konkrétnej siete. Najmä v prípade geograficky vzdialených sietí je potrebné vyriešiť *vzájomné prepojenie sietí*, aby komunikácia bola prenášané spoľahlivo, cez podľa možnosti minimálny počet sietí tretích strán a pokiaľ možno po najkratšej trase. Technické riešenie sa v tomto prípade z praktických dôvodov musí dohodnúť v čase uzatvárania ekonomickej dohody, neskôr sa zabezpečuje ťažšie.

5.4.3 Zraniteľnosti heterogénnych systémov

Heterogénne systémy sú také systémy, kde jednotlivé prvky nie sú produktom súčasného vývoja, čo môže mať negatívny vplyv na ich interoperabilitu. V praxi sa v prípade mobilných sietí vyskytujú dva varianty heterogénnych systémov. Prvým je *prepájanie prvkov rôznych dodávateľov*, druhým je *prepájanie prvkov rôznych generácií mobilných sietí*, aj keď boli skonštruované jedným výrobcom.

Kombinovanie prvkov náležiacich do rôznych generácií mobilných sietí sa vyskytuje najmä v prípade rozširovania existujúcej siete operátora novou technológiou. V praxi sa mu je možné niekedy vyhnúť, keď nové prvky často dokážu zastať funkcie viacerých generácií mobilných sietí súčasne a teda sa pôvodný prvok nahradí novým. Niekedy ale toto nie je možné a vtedy sa objavujú zraniteľnosti vychádzajúce z chýb v štandarde, nedokonalosti návrhu, prípadne nedostatočnosti testovania. V neskorších fázach je riešenie týchto zraniteľností technicky náročné a časovo a finančne nákladné.

Kombinovanie prvkov viacerých výrobcov sa vyskytuje väčšinou z ekonomických dôvodov a to typicky zo znižovania ceny kvôli konkurenčnému boju alebo z dôvodu nedostupnosti konkrétneho riešenia u niektorého dodávateľa technológie. Z rôznych dôvodov, ale v oboch prípadoch sa vyskytujú podobné problémy s interoperabilitou, vychádzajúce z voľnosti štandardu ktorý nestatočne definuje niektoré čiastkové riešenia či posupy[15], zámernej voľby nekompatibilných postupov či nedostatočného testovania kvôli neexistencii či nedostupnosti protikusu.

14 Druhým dôvodom býva riešenie problému synchronizovaného zlyhania, viz. kap. 5.4.1.

15 Voľnosť štandardu býva, najmä u skorších generácií mobilných sietí, zámerná, keď určité časti niesú definované najmä kvôli podpore inovácie vyplývajúcej z konkurenčného boja dodávateľov.

5.4.4 Zraniteľnosti systémov pracujúcich v reálnom čase

Systém pracujúci v reálnom čase (RTS, angl. „Real Time System“) je taký systém, kde správnosť výsledku záleží okrem faktickej korektnosti aj na termíne jeho dodania. V praxi tak RTS systém musí garantovane reagovať na vstup najneskôr v dopredu definovanom čase. Mobilná sieť ako systém využívajúci komunikačné procedúry založené na výmene správ medzi prvkami by z takéhoto prístupu profitovala. Definovaná reakčná doba na jednotlivé čiastkové požiadavky umožňuje stanoviť maximálnu dobu trvania celej procedúry.

Aby systém spĺňal požiadavky na prácu v reálnom čase, musí byť celý navrhnutý týmto spôsobom, od technických prostriedkov až po programové vybavenie. V praxi sa kvôli rýchlosti vývoja a cene často stavia na upravenom komoditnom hardware, ktorý sa práci v reálnom čase blíži, ale väčšinou ju nemôže garantovať. V špecifických prípadoch teda reakcie na požiadavky a následne celé signalizačné procedúry môžu trvať dlhšie ako požadovanú dobu, hoci väčšinou sa obslužný systém zdanlivo chová ako RTS. Pomôcť môže duplikácia dielčích zariadení a rozkladanie záťaže medzi ne, či paralelné vykonanie operácie voči viacerým duplikovaným prvkom, využitie prvého dodaného výsledku a stornovanie operácie na prvkoch ostatných, čo ale výrazne znižuje efektivitu. Skutočným riešením je len dôsledný návrh a následne podrobné testovanie prvkov ako RTS.

Ďalším zdrojom náhodnosti v chovaní je reakcia na vstup používateľa. Mobilná sieť musí byť schopná spracovávať takmer neobmedzenú množinu používateľských vstupov na rôznych úrovniach, takže špecifikovať a otestovať reakciu na všetky je zložité. Riešením by mohla byť formálna verifikácia či automatizovaný návrh obslužného systému.

Požiadavky na schopnosť mobilných sietí pracovať v reálnom čase aj na úrovni prenosu dát v používateľskej rovine a teda na to aby mobilné siete vkladali do realizovanej komunikácie minimálne oneskorenie boli identifikované už v počiatočných fázach nasadzovania paketovo orientovaného prenosu dát. To viedlo k teoretickému rozpracovaniu problematiky kvality služby a širokému nasadeniu týchto techník v mobilných sieťach. Pri okruhovo orientovanom prenose je latencia pomerne nízka, pretože po celej ceste transportu je zostavený okruh a teda vyhradené prostriedky pre realizovaný prenos. Paketý prenos dát trpí ale najmä oneskorením spôsobeným prideľovaním prostriedkov na rádiovom rozhraní mobilnej siete. Zatiaľ čo v druhej generácií mobilných sietí je vložené oneskorenie na úrovni nízkych jednotiek sekúnd, v generácii tretej ide o vyššie stovky milisekúnd a vo štvrtej generácii sa technológia dostáva na desiatky milisekúnd. Výrazný pokrok v tejto oblasti dosahujú siete piatej generácie, kde sa pri využití vyhradenej techniky URLLC (angl. „ultra reliable low latency communication“, vysoko spoľahlivá komunikácia s nízkym oneskorením) dosahuje oneskorenie na úrovni pevných sietí.

5.5 Zhrnutie kapitoly

Táto kapitola popisuje mobilnú bunkovú sieť na základe systémového prístupu, čiže štruktúrovane, na základe posúdenia podstatnosti jednotlivých častí, komplexne, hierarchicky a orientovane, so zameraním na cieľové chovanie.

Výsledkom je dokumentácia vysokoúrovňovej architektúry siete ako štruktúry systému a tiež vzťahy medzi jednotlivými prvkami pre zabezpečenie kvality služby realizovanej v sieti. Ďalej je analyzovaná interakcia mobilnej siete so svojím okolím, menovite kritickými infraštruktúrami, rádiovým prostredím a interakcia s používateľmi.

Vzhľadom k tomu, že mobilná sieť ako telekomunikačná infraštruktúra existuje preto, aby sa cez ňu realizovali služby, sú analyzované možné druhy služieb či ich požiadavky a zhodnotené možnosti ich realizácie mobilnou sieťou. Služby mobilných sietí sa z hľadiska častí siete, ktoré za ne zodpovedajú, rozdeľujú na služby realizované v okruhovo prepínanej doméne, všeobecné dátové služby realizované v paketovo prepínanej doméne a služby integrované do siete, ktoré sú realizované v rámci signalizačného komunikačného kanála mobilnej siete. Takéto rozdelenie umožňuje službám apriórne priradiť vlastnosti, pretože tie vychádzajú z technickej špecifikácie správania jednotlivých týchto častí siete.

Mobilné siete si prešli vývojom, ktorý má nezanedbateľný vplyv na ich aktuálnu štruktúru a vlastnosti a preto je uvedená tiež podkapitola mapujúca postupný vývoj generácií mobilných sietí od prvých rádiových systémov pre obojsmernú komunikáciu až po aktuálne inštalované komunikačné zariadenia.

V neposlednom rade je identifikované, že mobilné siete majú určité všeobecné vlastnosti vychádzajúce z ich konštrukcie, ktoré sú spoločné s inými systémami zdieľajúcimi čiastkové požiadavky či technické rozhodnutie. Z týchto vlastností vychádzajú možné systémové zraniteľnosti a tak je ich analýze venovaný priestor. Konkrétne ide o možné zraniteľnosti mobilných sietí ako systémov využívajúcim technickú zálohu pre zvýšenie spoľahlivosti, ako geograficky rozľahlých systémov kde sa musí prihliadať na dobu odozvy, ako systémov heterogénnych kde je nutné zabezpečiť interoperabilitu rozdielnych prvkov a ako systémov pracujúcich v reálnom čase, ktoré musia v reakcii na vstup okrem faktickej správnosti výsledku tento dodať najneskôr v definovanom čase aby ho bolo možné zmysluplne využiť.

Výsledky analýzy na základe systémového prístupu sú vstupom do rôznych analýz rizík, ktoré sú primárnym cieľom práce.

6 Analýza rizík mobilných sietí

Analýza rizík vychádza zo systémového prístupu k problematike a spočíva v identifikácii požiadaviek na jednotlivé súčasti a okolie systému, ich zástupnosťou či možnosťou náhrady a dopadmi ich zníženej dostupnosti či výkonnosti na schopnosť celku plniť definované funkcie.

6.1 Mobilná sieť ako chránené aktívum

V prípade mobilných bunkových sietí je zdrojom ohrozenia človek, či sa jedná o úmyselný zásah, pochybenie, či nedostupnosť personálu, ďalej príroda vo forme akútneho zásahu – živelná pohroma, ale tiež dlhodobého pôsobenia v zmysle degradácie prvkov, do určitej miery tiež legislatívne prostredie kde dochádza k protichodným požiadavkám či geopolitická situácia – napr. nedostupnosťou náhradných dielov a know-how a v neposlednom rade samotné technické vybavenie, jeho chyby v hardware a software častiach degradujúce okolité prvky či dočasne obmedzujúce ich funkcie. V súvislosti so svojím okolím prvky mobilnej siete vyžadujú elektrické napájanie a keďže samostatne je sieť schopná fungovať len v obmedzenom režime, je tiež nutné napojenie na iné telekomunikačné siete. Všetky tieto väzby vychádzajú z aplikácie systémového prístupu.

Druhý možný pohľad je hľadisko životného cyklu technického vybavenia komunikačnej siete. Identifikácia zdrojov ohrozenia a do určitej miery aj zraniteľností vychádza zo systémového prístupu a tieto množiny sa počas životného cyklu príliš nemenia, zameranie na jednotlivé fázy životného cyklu ale umožňuje lepšie identifikovať scenáre nebezpečia a následné nápravné opatrenia.

Vzhľadom k tomu, že zdroje nebezpečia ovplyvňujú mobilnú sieť počas celej doby života a to zhruba v rovnakom zložení po celú dobu, ale v jednotlivých fázach s inou intenzitou, môžeme pre vysoko úrovňový pohľad s výhodou použiť pre formálny popis upravený tzv. „formulár experta“ metódy UMRA[16]. Zvyšok metódy je technicky použiteľný tiež, ale v prípade použitia len jedného hodnotenia namiesto celej sady expertných posudkov využitie metódy nie je príliš výhodné. Uvedený „formulár experta“ je v Tab. 2, kde hlavným výstupom sú koeficienty dôležitosti, čo sú relatívne váhy jednotlivých zdrojov nebezpečia a tiež fáz životného cyklu. Z analýzy vidno, že pre mobilnú bunkovú sieť vo funkcii kritickej infraštruktúry je najvýznamnejším zdrojom nebezpečia motivovaný útočník, nasledovaný geopolitickou situáciou. Z pohľadu životného cyklu zase vychádza ako najdôležitejšia fáza prevádzky, nasledovaná údržbou a hľadaním závady.

16 Metóda UMRA je podrobne popísaná autorom, prof. Tichým, v [10].

Tab. 2: Koeficienty nebezpečia pre fázy životného cyklu mobilnej siete

Fáza životného cyklu	**Zdroj nebezpečia**							**Koeficient dôležitosti**
	Antropogénny			Prírodný		Technický		
	Útočník	Obsluha	Geopolitika	Živel	Dlhodobé pôsobenie	Súčasti	Okolie	
Projektovanie	3	0	2	0	0	1	1	0,08
Výroba	3	0	2	1	0	0	2	0,09
Doprava	2	1	2	1	0	0	0	0,07
Montáž a inštalácia	2	2	1	1	0	1	1	0,09
Konfigurácia	2	2	1	0	0	2	1	0,09
Prevádzka	3	2	2	2	1	2	3	0,17
Údržba	2	1	3	2	2	2	1	0,15
Hľadanie závady	2	3	2	1	1	3	1	0,15
Vyradenie z prevádzky	2	2	1	0	0	1	0	0,07
Likvidácia	3	0	1	0	0	0	0	0,05
Koeficient dôležitosti	0,27	0,15	0,19	0,09	0,05	0,14	0,11	

Ďalej pokračujeme podrobnejšou analýzou, kde sa jednotlivým fázam a zdrojom nebezpečia budeme venovať podľa ich koeficientov dôležitosti z Tab. 2. Pre nadväzujúcu analýzu použijeme prístup odvodený od toho zavedeného harmonizovanými normami pre funkčnú bezpečnosť, pretože pracuje s vhodným aparátom posudzovania kde sa samostatne hodnotia aspekty dopadu S, početnosti a doby trvania A, možnosti vyvarovania sa nebezpečiu E a pravdepodobnosti výskytu W. Jedná sa vlastne o rozšírenie systémovej varianty metódy FMEA [10], s pridaním parametru doby trvania zraniteľnosti, kde sa prihliada k tomu, že náchylnosť k niektorému riziku môže byť prítomná len za určitých okolností. Škála pre hodnotenie aspektov rizík mobilných bunkových sietí je uvedená v Tab. 3, táto stupnica je upravená pre hodnotenie vlastností kritickej infraštruktúry namiesto funkčnej bezpečnosti zariadenia. Výsledná hodnota rizika je potom produktom (vynásobením hodnôt jednotlivých aspektov) a teda sa jedná o nelineárnu škálu, môže slúžiť len k určeniu poradia veľkosti rizika, nie k jej absolútnemu porovnaniu.

Tab. 3: Stupnica pre hodnotenie aspektov rizík mobilných bunkových sietí

Kategória	**Značka**	**Škála**	**Vysvetlenie**
Dopad	S	1	Mierne obmedzenie funkcie, zhoršenie kvality služieb
		2	Závažnejšie lokalizované obmedzenie funkcie, pozorovateľné výpadky
		3	Celkový lokálny výpadok trvajúci niekoľko dní / pozorovateľné výpadky naprieč celou sieťou
		4	Významné obmedzenie funkcie s výpadkom trvajúcim niekoľko dní
Doba trvania	A	1	Vzácne krátkodobé trvanie zraniteľnosti
		2	Častá až trvalá zraniteľnosť
Odvrátenie	E	1	Možné za určitých podmienok
		2	Ťažko možné
Pravdepodobnosť výskytu	W	1	Veľmi malá
		2	Malá
		3	Pomerne vysoká

Po identifikácii, analýze a posúdení rizík nasleduje návrh nápravných opatrení. Pretože jednotlivé opatrenia majú spravidla vplyv len na jeden z aspektov rizika, použije sa ich často niekoľko v kombinácii. Analýza rizík s hodnotením, navrhnutými opatreniami a novou hodnotou rizika po ich aplikácii je uvedená v tabuľke v prílohe. Vzhľadom na úroveň detailov, zvolenú tak aby bolo možné pokryť mobilnú sieť komplexne, je realizovaná vysoko-úrovňová analýza, ktorá by v praxi bola doplnená detailnejšou analýzou pre jednotlivé prvky komunikačnej siete, zameranou na ich špecifiká, konfiguračné možnosti, geografické a technické okolie a z toho vyplývajúce hrozby a zraniteľnosti.

6.2 Mobilná sieť ako zdroj ohrozenia

Akákoľvek kritická infraštruktúra musí pre naplnenie svojej funkcie byť primerane bezpečná pre svoje okolie, inak by ju nebolo možné používať a zase naopak, nikdy by nemala potenciál stať sa kritickou infraštruktúrou. Z tohto dôvodu je nutné analyzovať aj vplyvy prevádzky kritickej infraštruktúry na svoje okolie.

Mobilné siete sú tvorené technickými zariadeniami na ktoré sa aplikujú príslušné bezpečnostné normy, napr. [13]. Zariadenia nespĺňajúce takéto normy nie je vôbec možné inštalovať a používať, preto kvôli zjednodušeniu analýzy tieto aspekty vynecháme. Nakoniec ich vplyvy na okolie nie sú odlišné v porovnaní s prevádzkou iných technických zariadení.

Na takto formulovaný problém sa nejaví priamo aplikovateľná žiadna zo známych formálnych metód analýzy rizika. Z toho dôvodu sa analýza rizika vykoná štruktúrovane na základe preverovania jednotlivých častí mobilnej siete a ich väzieb na okolie siete. Pri analýze sa využijú aplikovateľné čiastkové postupy z analýz FMEA a HRA.

Jadro siete je typicky inštalované v klimatizovanej serverovni, kam nemá prístup bežná populácia. Veľkosť ani hmotnosť takej inštalácie nie sú ani pre pokrytie značnej geografickej oblasti veľké, prevádzka spotrebúva elektrickú energiu a generuje teplo a kvôli chladeniu hluk. Žiadny z týchto aspektov nie je odlišný od prevádzky iných výpočtových či komunikačných prostriedkov, takže je možné konštatovať, že jadro mobilnej siete nie je zdrojom neprimeraných ohrození svojho okolia.

Transportná infraštruktúra mobilnej siete je v zastavaných oblastiach vedená typicky optickými vláknami či metalickými vedeniami, s využitím šácht a trubíc zdieľaných s inou komunikačnou infraštruktúrou. V riedko osídlených oblastiach sa spoje väčšinou vedú bodovými spojmi. Tie vyžadujú priamu viditeľnosť a teda typicky neožarujú ľudí, faunu ani flóru. Môže dôjsť ku krátkodobému vystaveniu pohybujúcich sa objektov žiareniu, ale vyžarované výkony nie sú veľké a vplyv by mal byť minimálny. Dlhodobé pôsobenie je vylúčené, taký dej by spôsobil nefunkčnosť spoja. Z estetického a environmentálneho hľadiska je vplyv transportnej infraštruktúry malý až neexistujúci. V určitých prípadoch môže byť nutné vybudovať nový spoj, čo si vyžaduje inštalačné a niekedy stavebné práce, prípadne výkopy a uloženie vedení. V takom

prípade je vhodné minimalizovať dobu prác i zásah do okolia a v prípade nutných zásahov obnoviť okolie prác čo najviac v súlade s pôvodným stavom či s iným revitalizačným zámerom. Táto možnosť zásahov, najmä v prípade životného prostredia, je najväčšou potenciálnou hrozbou transportnej infraštruktúry voči okoliu mobilnej siete.

Asi najviac problematickou časťou mobilnej siete je rádiová prístupová sieť, špeciálne základňové stanice. Tie ako vysielače elektromagnetického žiarenia majú potenciálny vplyv na svoje okolie, technické i prírodné. Maximálne úrovne žiarenia sú regulované[17], zároveň reálne využívané úrovne sa postupne znižujú. To je spôsobené viacerými faktormi, jednak je to požiadavka na predĺženie pohotovostnej doby zariadenia pri napájaní z batérie, čo má vzájomný vplyv s postupným nárastom šírky komunikačného kanálu. Ďalej kvôli zdieľaniu prenosovej kapacity bunky všetkými obsluhovanými používateľmi a kvôli presunu prenosu do stále vyšších frekvencií (tiež súvisí s potrebou zvyšovať šírku kanálu), čo znamená horšiu priestupnosť signálu prostredím sa bunky v každej generácii sietí zmenšujú. Využívané komunikačné kanály sa tiež presúvajú na frekvencie, ktoré boli desaťročia používané na šírenie televízneho signálu a to s výrazne vyššími vysielacími výkonmi, čiže žiarenie na týchto frekvenciách zrejme nie je pre ľudí a prírodu príliš nebezpečné. Napriek tomu existujú jedinci citliví na elektromagnetický smog i keď zdá sa v menšej miere ako napríklad svetelné znečistenie a podobné skryté vplyvy.

Ďalším negatívom základňových staníc je nutnosť ich inštalácie v prostredí kde sa pohybujú používatelia, čo naopak zmenšovanie veľkosti bunky zhoršuje. Niektorí ľudia môžu takéto inštalácie považovať za neestetické, čo je ale subjektívna záležitosť ktorá sa zle vyhodnocuje. Rozhodne je ale vhodné akékoľvek technické zariadenia integrovať do prostredia spôsobom, ktorý nie je prehnane rušivý.

Nutnou súčasťou mobilnej siete sú aj účastnícke terminály. Tie sú zdrojom podobného ohrozenia elektromagnetickým žiarením ako základňové stanice, avšak z pohľadu pôsobenia na človeka mávajú vyšší dopad, pretože sú prevádzkované v tesnej blízkosti a teda vysielaný výkon je výrazne menej tlmený vzdialenosťou. Pôsobenie terminálov mobilných sietí na človeka je priebežne skúmané, prípady keď nevzniká tepelné pôsobenie na tkanivo sa považujú za dostatočne bezpečné. Z tohto dôvodu je vhodné zariadenia pri používaní držať ďalej od mäkkých tkanív, či limitovať dobu expozície. Dobrým riešením sa javí používanie súprav na telefonovanie bez použitia rúk. Okrem vplyvu žiarenia sú terminály aj určitou formou osobného asistenta, často teda obsahujú dôverné informácie o používateľovi, zároveň sú kvôli veľkosti a tomu že sa nosia so sebou náchylné na stratu či odcudzenie. Ďalej často bývajú trvalo pripojené k sieti internet a stav bezpečnostných aktualizácií proti kybernetickým zraniteľnostiam nebýva dobrý, aj keď v poslednej dobe sa začal výrazne zlepšovať. Nové mobilné terminály zvyčajne používajú silnú kryptografiu ako prostriedok zabezpečenia dôvernosti uložených dát a zvyknú podporovať

17 Jedná sa o rodinu noriem ČSN ETSI EN 300000 – 399999, konkrétna norma závisí na použitej frekvencii, pričom pásma využívané mobilnými sieťami sú pokryté viacerými. ETSI – angl. „European Telecommunication Standards Institute“, európsky inštitút pre telekomunikačné štandardy.

možnosť lokalizácie zariadenia či dokonca vzdialeného zmazania dát po strate či odcudzení. Problémom môže byť triviálna metóda autentifikácie používateľa, keď útočník túto prekoná pred vykonaním uvedených bezpečnostných opatrení, čím získa plný prístup a kontrolu nad zariadením. V prípade chýbajúcej zálohy dát majú uvedené riziká dopad aj na dostupnosť dát.

Tiež je potrebné zamerať sa na makroergonomické aspekty technológie mobilných sietí. Vysoká rozšírenosť mobilných terminálov v populácii, takmer bez ohľadu na vek, v kombinácii so stálou dostupnosťou internetového pripojenia môže mať negatívny vplyv na používateľov. U niektorých mobilný telefón nahrádza bežný sociálny kontakt až do miery, že interakcia s mobilným telefónom je preferovaná pred interakciou s iným človekom. Ďalej dlhodobé vystavenie neustále dostupnému zdroju zábavy má negatívny vplyv na okamžitú pozornosť a schopnosť sústrediť sa, ale tiež môže vyvolávať neochotu pracovať na ťažšie dosiahnuteľných cieľoch, či takých čo vyžadujú dlhodobé úsilie. Mobilné siete a súvisiace technológie rozhodne majú potenciál ovplyvniť ľudskú spoločnosť a vplyvy nemusia byť len kladné.

6.3 Zhrnutie kapitoly

Táto kapitola sa venovala analýze rizík súvisiacich s mobilnými sieťami, kde tieto vystupujú ako v úlohe chráneného aktíva, tak v úlohe zdroja ohrozenia pre svoje okolie. Z pohľadu pôsobenia mobilných sietí ako kritickej infraštruktúry majú väčší priamy dopad hrozby pôsobiace na infraštruktúru, ale najmä z dlhodobého hľadiska sa ani hrozby voči okoliu nesmú podceňovať.

Pri analýze rizík boli využité formálne metódy UMRA a FMEA, ale pretože sa jedná o všeobecné metódy, boli modifikované pre problematiku mobilných sietí. Analýza ukazuje, že je z pohľadu rizík potrebné sa zaoberať najmä fázami prevádzky, údržby a diagnostiky mobilných sietí, čo sú našťastie z pohľadu prevádzkovateľa najľahšie ovplyvniteľné oblasti. Podobne ohľadom zdrojov ohrozenia je najväčšou hrozbou vonkajší útočník a s odstupom nasledujú geopolitické hrozby a hrozby od obsluhy, teda ľudský faktor. V rámci analýzy FMEA sa ukazuje, že riziká v prípade mobilných sietí je možné pomerne úspešne riadiť pomocou bezpečnostných opatrení.

Na druhú stranu menej formálny prístup, založený na systematickom posúdení interakcie prvkov siete s okolím, bol použitý v prípade identifikácie hrozieb od mobilnej siete voči okoliu. Výsledkom je kvalitatívny popis hrozieb, príčin a možných dopadov, čo ukazuje že aj takýto prístup môže viesť k potrebným či uspokojivým výsledkom.

Analýza rizík je dôležitým aspektom riadenia rizík a predpokladom návrhu bezpečnostných opatrení. Pre reálne nasadenie riadenia rizík je ale nutné výsledky získané analýzami overiť v praxi a integrovať do plánov krízovej pripravenosti, k čomu zároveň po ich vykonaní sú dostupné všetky potrebné podklady.

7 Diskusia výsledkov

V tejto kapitole je uzatvorená analýza a diskusia dosiahnutých výsledkov. Podkapitola 7.1 sa venuje overeniu analyzovaných metód pre technickú diagnostiku mobilných bunkových sietí v praktickom nasadení komerčných sietí. Ďalej podkapitola 7.2 pojednáva o krízových plánoch mobilnej siete a ich previazanosťou s platnou legislatívou.

7.1 Overenie metód diagnostiky mobilných sietí v praxi

Pre praktické overenie metód diagnostiky mobilných sietí boli realizované merania v reálnych komerčných mobilných sieťach, kde diagnostické ciele vyplývali z prezentovaných problémov jednotlivých operátorov mobilných sietí.

7.1.1 Analýza úspešnosti a výkonu paketovo orientovaných dátových služieb

Meranie bolo realizované na jednom rádiovom subsystéme mobilnej siete, riadeným jedným RNC (angl. „Radio Network Controller“ – kontrolér rádiovej siete); dáta pre výkonnostnú analýzu boli získané pomocou pasívnej sondy rozhraní mobilnej siete. Zámerom bolo vyhodnotenie parametrov ako obojcestná doba odozvy RTT a jednocestné oneskorenie pre služby realizované v používateľskej rovine a tiež časovanie a pomer úspešnosti procedúr riadiacej roviny.

Keďže meranie bolo realizované v spolupráci s firmou EXFO ktorá dodala meracie systémy, dáta boli zachytávané využitím pasívnej sondy rozhraní EXFO PowerHawk, počas siedmych súsledných dní. Zachytávanie dát používateľskej roviny bolo obmedzené na dve hodiny denne počas hlavnej prevádzkovej doby určenej pre analyzovaný segment siete. Celkové zachytené množstvo dát bolo 7TB. Zachytené boli dáta v GTP-U tuneli medzi RNC a GGSN (angl. „Gateway GPRS Support Node“, brána do paketovej siete), t.j. na tzv. „Direct Tunnel“[18] rozhraní. Dáta riadiacej roviny boli zachytávané na rozhraní Iu-PS medzi RNC a SGSN (angl. „Serving GPRS Support Node“, riadiaci prvok pripojenia), nepretržite počas celej analyzovanej doby, t.j. 24x7 hodín a neskôr spracované pomocou analyzátora EXFO TravelHawk Pro. Do siete sa pasívna sonda pripájala cez existujúcu nízko-úrovňovú dohľadovú infraštruktúru Gigamon,

18 Rozhranie „Direct Tunnel“ je priame spojenie medzi prvkami RNC a GGSN pre prenos dát používateľskej roviny namiesto dvoch spojení v trase RNC-SGSN-GGSN podľa pôvodnej špecifikácie 3GPP, čo umožňuje zníženie latencie odbúraním potreby odpúzdrovať a znovu zapúzdrovať dáta a je možné preto, že prvok SGSN do používateľských dát nezasahuje. Nevýhodou je nutnosť spojenia 1) všetkých použitých RNC, ktorých je v reálnej sieti výrazne viac ako SGSN, 2) na všetky potrebné brány GGSN, cez ktoré môže používateľská komunikácia tiecť, čo kladie väčšie nároky na prvky RNC a GGSN. Komunikácia riadiacej roviny stále prebieha štýlom RNC-SGSN-GGSN.

kde boli odbočené virtuálne okruhy prenášajúce požadované spoje. Novinkou z pohľadu diagnostických zvyklostí bolo zaradenie vyhodnocovania štatistických momentov vyššieho rádu pri vyčíslovaní doby trvania jendotlivých procedúr, ako je popísané v kap. 4.3.1. Tento postup umožnil identifikáciu takých kľúčových výkonnostných indikátorov, ktoré s vyššou pravdepodobnosťou ukazovali na možný problém v sieti, čo v prípade použitia len aritmetického priemeru, ako bolo dovtedy zaužívané, nešlo. Realizované výsledky dopĺňali iné existujúce meranie metódou drive-testing, s tým rozdielom, že lepšie zodpovedali spätnej väzbe získavanej operátorom mobilnej siete od používateľov.

7.1.2 Porovnanie KPI v rádiovej prístupovej sieti odlišných dodávateľov technológie

Meranie malo za cieľ verifikovať podmienky pre akceptačné testovanie inštalovanej siete základňových staníc, ktoré mali nahradiť predtým používanú technológiu iných výrobcov. Obmena technológie sa vykonávala po častiach a vždy sa vykonali rozsiahle testy pred a po výmene v konkrétnej oblasti. Porovnávané boli dosahované výsledky výkonu a výkonnosti pred a po výmene ako aj rozdiely vo výsledkoch výkonnosti rádiovej siete medzi rôznymi geografickými oblasťami v jednom čase, najmä pre určenie zmeny záťaže siete kvôli korekcii nameraných dát.

Základňové stanice jednotlivých výrobcov boli primárne dohľadované systémami dodanými týmito výrobcami. Pretože vzniklo podozrenie na inkonzistenciu vyčíslovania KPI, vyvstala potreba toto preskúmať a určiť korigovanú metodiku porovnávacích testov. Pre porovnanie výkonnosti základňových staníc jednotlivých výrobcov preto boli paralelne nasadené pasívne sondy rozhraní.

Z údajov získaných sondami a ich porovnaním s výsledkami z jednotlivých dohľadových systémov bolo zistené, že dohľadové systémy rôznych výrobcov počítajú identicky označované KPI rôzne, najčastejšie ako súčet rôznych množín čiastkových výkonnostných indikátorov[19]. Takýmto spôsobom boli preverené všetky procedúry riadiacej roviny a testy v používateľskej rovine, ktoré boli súčasťou akceptačného testovania. Výsledkom analýzy boli nové vzorce pre jednotlivé KPI tak, aby tieto boli vyhodnotené identicky pre základňové stanice všetkých výrobcov.

Sekundárnym výsledkom boli zaujímavé štatistiky porovnávajúce nízkoúrovňové indikátory výkonnosti základňových staníc, napr. boli zistené rozdiely v majoritných dôvodoch zlyhania jednotlivých procedúr riadiacej roviny medzi výrobcami. U jedného výrobcu bol identifikovaný problém s uvoľňovaním pridelených časových slotov na rádiovom rozhraní za určitých podmienok, čo časom viedlo k vyčerpaniu prostriedkov napriek tomu, že reálne

19 Príkladom môže byť výrobca, ktorý pre výpočet počtu zlyhaných pokusov pre vytvorenie pripojenia k paketovo prepínanej sieti používal súčet len niektorých dôvodov zlyhania, pričom iné ignoroval.

nedochádzalo k ich využitiu. V inom prípade bolo zistené, že jedno riešenie trpelo veľmi častým rozpadom už nadviazaného spojenia kvôli problémom s časovaním procedúr riadenia komunikácie napriek tomu, že v ostatných KPI dosahovalo veľmi vysokú spoľahlivosť. Zaujímavý bol problém porovnania dvoch systémov, kde jeden vykazoval vysokú úspešnosť procedúr ale dlhšiu dobu ich trvania, druhý mal úspešnosť zníženú, ale procedúry boli dokončené v katšom čase. Druhý typ vykazoval lepšie výsledky pri meraní metódou drive-testing pred uvedením do prevádzky, ale pri bežnom reálnom vyťažení poskytoval výrazne menej kvalitné služby používateľom. Nasadenie pasívnych sond rozhraní umožnilo detailne popísať prebiehajúce deje a identifikovať príčiny tohto nesúladu.

7.1.3 Porovnanie jednotlivých variantov Circuit Switched Fallback

Technológia CSFB, prenos hlasového hovoru cez okruhovo spínanú doménu staršej generácie paralelne vybudovanej mobilnej siete, v prípade chýbajúceho pokrytia či nemožnosti zabezpečiť kvalitatívne požiadavky služby v čisto paketovo spínanej mobilnej sieti umožňuje postupné nasadzovanie hlasového volania cez paketovo prepínané mobilné siete, tzv. VoLTE, bez nutnosti vybudovania kompletného pokrytia a nutnosti VoLTE podporovať v každej bunke. Techniky CSFB existuje viacero variantov, najmä z pohľadu využívanej generácie okruhovo prepínanej siete, smere prevodu hovoru a konfigurácie mobilnej infraštruktúry, konkrétnych prítomných prvkov a prepojení medzi nimi.

V rámci merania bola okrem časovania procedúr prevodu hlasového hovoru v jednotlivých variantoch vykonaná tiež hlbšia analýza príčin degradácie v prípade variantov s horšími výsledkami. Ukázalo sa, že v tejto úlohe sú rozdiely nielen medzi prvkami pre prepínanie hovorov ale tiež subsystémami základňových staníc, ktoré nešli vždy vyriešiť aktualizáciou software. Systematicky vyššie hodnoty trvania procedúr riadiacej roviny pri okruhovo spínanej službe sa v prípade kombinácie s paketovo prepínanou sieťou a prenosu hlasového hovoru do nej prejavili na úspešnosti takejto operácie.

7.1.4 Akceptačné testovanie VoLTE rôznymi diagnostickými nástrojmi

VoLTE je technológia pre prenos hlasových hovorov paketovo spínanou mobilnou sieťou so zabezpečením kvality služby. Takéto riešenie umožňuje realizáciu hlasových hovorov v mobilných sieťach, ktoré nemajú podporu prenosu okruhovo spínaných dát, bez potreby paralelnej prevádzky mobilnej siete staršej generácie. Pre nasadenie technológie VoLTE v komerčnej sieti je potrebné najprv verifikovať výkonnostné charakteristiky takéhoto riešenia, čo sa deje akceptačným meraním. Toto meranie je v podstate zovšeobecneným variantom

merania popísaného v kap. 7.1.3, so zvýšeným zreteľom na hovor čisto realizovaný v paketovo spínanej mobilnej sieti a zameraný viac na analýzu výkonu než na kompletnú diagnostiku. Výrazným rozšírením je využitie maximálneho množstva diagnostických metód nevyžadujúcich prístup k infraštruktúre mobilnej siete pod správou tretej strany, čiže metódy drive-testing, agentov na používateľských koncových zariadeniach, pasívnych sond rozhraní medzi jednotlivými kľúčovými prvkami siete a v obmedzenej miere tiež štatistík získaných z dohľadového subsystému mobilnej siete.

Konečným výsledkom merania boli samozrejme výkonnostné parametre realizovaných hovorových služieb, podstata však ležala v porovnaní jednotlivých diagnostických metód a výbere najvhodnejších možností pre konkrétne podmienky. Výhody a nevýhody metód boli popísané v kap. 4.2, ich aplikovateľnosť do veľkej miery vychádza z ich technickej podstaty, situáciu ale komplikujú rôzne administratívne obmedzenia. Pre akceptačné testovanie je nutné využitie aktívnych metód, pasívne metódy sú ale vhodným doplnením pre prípadnú hlbšiu analýzu a hľadanie príčin v prípade nedostatočnej výkonnosti. Ďalšou, kľúčovou, výhodou súčasného využitia pasívnych metód pri akceptačných testoch je možnosť následného monitorovania v dobe pilotnej prevádzky, čo umožní overiť výkon pri zaťažení siete bežnou používateľskou premávkou a jeho vzťah k výkonu zisteného pomocou aktívnych, do určitej miery syntetických, testov.

7.2 Plán krízovej pripravenosti mobilnej siete

Plán pripravenosti na krízové situácie alebo tiež plán krízovej pripravenosti vychádza a snaží sa reagovať na riziká ohrozujúce mobilnú sieť počas svojho životného cyklu, ako boli identifikované vo fáze analýzy rizík. Zmyslom takéhoto plánu je zvýšenie prevádzkyschopnosti infraštruktúry pri vzniku mimoriadnej situácie. Koordinátorom krízového plánovania v ČR je podľa zákona o krízovom riadení [4] Hasičský záchranný zbor ČR.

Plán krízovej pripravenosti je založený na dvoch nosných častiach [15]. Prvou je proaktívna bezpečnosť, teda súbor bezpečnostných opatrení, ktoré majú za cieľ zabrániť potenciálnej hrozbe v materializácii do skutočnej. Druhou je reaktívna bezpečnosť, teda plány odozvy na krízovú situáciu a následne plány obnovy po krízovej situácii. Rozdelenie reaktívnej bezpečnosti na dve súsledné podčasti vychádza z praxe a rozdielnosti ich úloh. Zatiaľ čo plány odozvy majú za cieľ stabilizovať situáciu, zabrániť šíreniu a ďalším škodám, pričom je dôležitá rýchlosť reakcie, plány obnovy sú zamerané na navrátenie dlhodobej funkcie, odstránenie následkov a revitalizáciu okolia, čo sú činnosti časovo náročné a často vyžadujúce ďalšie prípravy. Krízové plánovanie má širšiu pôsobnosť ako havarijné plánovanie, pretože rieši nielen bezpečnosť konkrétneho zariadenia, ale aj dôsledky na jeho potenciálne široké technické a najmä sociálne okolie. Na riešenie rozsiahlych mimoriadnych udalostí, spôsobených či už prírodnými alebo antropogénnymi faktormi, havarijné plánovanie nestačí.

Centrálnym prvkom krízovej pripravenosti je súhrn bezpečnostných opatrení. Z praktického hľadiska teda životný cyklus riadenia mimoriadnych situácií môžeme rozdeliť na fázu prípravy na mimoriadne situácie, kedy sú bezpečnostné opatrenia vytvárané, fázu reakcie na mimoriadnu situáciu, kedy sú bezpečnostné opatrenia aplikované a fázu kontroly, kedy sú proaktívne a reaktívne bezpečnostné opatrenia analyzované, je vyhodnocovaná ich účinnosť a sú zlepšované. Krízový plán stavia na analýze možných rizík, hrozieb a zraniteľností, určuje organizačnú štruktúru a zodpovednosť osôb za bezpečnostné opatrenia. Jeho operatívna časť zase definuje aplikované opatrenia a spôsob ich realizácie, plán dodávok nevyhnutného materiálu a služieb, spôsoby komunikácie s kooperujúcimi subjektami krízového plánovania či plány riešenia konkrétnych druhov nebezpečí.

V prípade kritickej infraštruktúry nie je možné pripustiť stav nemožnosti či neekonomickosti obnovy funkcií [15]. Ak by takáto situácia hrozila, je nutné vytvoriť náhradné technické riešenia zastávajúce rovnaké funkcie. Pripravenosť kritickej infraštruktúry na krízové situácie spočíva nie len v schopnosti udržania funkcie či včasnej obnovy, ale najmä v zamedzení negatívnych dopadov na okolie.

Mobilné komunikačné siete teda potrebujú plány pre urýchlenú obnovu v prípade havárie, stavu nebezpečia či mimoriadnej udalosti takým spôsobom, aby v minimálnej možnej miere a po čo najkratšiu dobu bola obmedzená ich funkcia, teda poskytovanie komunikačných služieb. Konkrétne kroky vychádzajú zo spôsobu a rozsahu poškodenia a môžu siahať od optimalizácie prevádzkových parametrov, cez rekonfiguráciu topológie siete až po inštaláciu nových dočasných či trvalých prvkov siete. V realizácii nápravných opatrení po narušeniach funkcie všetkých typov pomáha to, že ekonomický záujem prevádzkovateľa siete je prakticky vždy totožný so záujmom verejným a spoločenským a to je urýchlené obnovenie funkcie. Nutná prevaha legislatívy je vlastne len u obnove prostredia v prípade, že zdrojom havárie bolo zariadenie mobilnej siete a došlo ku poškodeniu okolia.

7.3 Zhrnutie kapitoly

Táto kapitola sa zaoberala diskusiou v práci dosiahnutých výsledkov, najmä tých častí ktoré neboli dostatočne diskutované v priebehu práce. Jedná sa najmä o praktické overenie analyzovaných metód v reálnych mobilných sieťach komerčných operátorov, kde sú sumarizované silné stránky metód ktoré boli z výhodou využité. Druhou časťou je diskusia pripravenosti mobilných sietí na krízové situácie, kde sa na základe legislatívnych požiadaviek definujú potrebné organizačné a technické opatrenia pre riadenie mimoriadnych situácií súvisiacich s mobilnými sieťami. Diskusia je založená ako na požiadavkách praxe, tak na analýzach realizovaných v predchádzajúcich kapitolách. Výsledkom diskusie je, že v práci navrhnuté metódy a postupy sú prakticky použiteľné, samozrejme pri rešpektovaní ich vstupných požiadaviek, štrukturálnych obmedzení a v neposlednom rade aj ekonomickej stránky.

8 Záver

Predkladaná práca sa venuje problematike prevádzky mobilných sietí v roli kritickej infraštruktúry a teda možnosti zabezpečenia kritických mobilných telekomunikačných služieb, nie bez ohľadu ale naopak najmä s prihliadnutím na stav okolia a možné riziká.

Každá práca musí byť zasadená do existujúceho prostredia, vychádzať z dobového stavu problematiky a úrovne znalostí a technickej praxe. V prípade prevádzky kritickej infraštruktúry, čo je problematika legislatívne regulovaná, je nutné začať analýzou legislatívneho rámca, špecifikujúceho obor. Vzhľadom na pochopiteľné zameranie legislatívy na všeobecné charakteristiky prevádzky kritickej infraštruktúry, je tiež potrebné vychádzať z oborových noriem a zvyklostí v obore.

Pre dosiahnutie cieľov práce, ako pri riešení akéhokoľvek netriviálneho problému, bola použitá kombinácia mnohých metód. V prvom rade sa jedná o zostavenie popisu mobilnej siete pomocou systémového prístupu, teda štruktúrovane a s prihliadnutím na podstatné znaky a vlastnosti a rešpektovaním štruktúry a vzťahov vnútorných aj vonkajších. Ďalej sú dôležité metódy pre analýzu rizík a posúdenie bezpečnosti technických systémov, či už obecné z oblasti inžinierstva rizík, tak metódy špecifické v praxi technickej správy mobilných sietí. Všetky metódy sú v práci charakterizované a je posúdená ich vhodnosť pre riešenie jednotlivých problémov mobilných sietí, či zabezpečovania a zvyšovania kvality služby nimi ponúkaných.

Viaceré z metód sú využité pri analýze rizík, prípadne overené v praxi aplikáciou na komerčné mobilné siete rôznych generácií a inštalovaných v rôznych krajinách. Analýza rizík sa okrem rizík ohrozujúcich mobilné siete zameriava aj na hrozby ktoré vyplývajú od mobilných sietí vzhľadom k ich okoliu, pretože kritická infraštruktúra poskytuje služby spoločnosti a jedincom a teda musí byť v prvom rade bezpečná na používanie.

Dôležitou požiadavkou na kritickú infraštruktúru je, aby fungovala nie len za normálneho stavu, ale aj, a to azda špeciálne, v dobe mimoriadnych udalostí či stave nebezpečia. V tomto ohľade je potrebné vypracovať plány krízovej pripravenosti pre reakciu na nebezpečenstvo, poruchy a havárie a obnovenie funkcie v čo najkratšej dobe. Tomu pomáha fakt, že tieto požiadavky sa prakticky kryjú s ekonomickými záujmami prevádzkovateľa siete.

Mobilná sieť je z pohľadu teórie aj praxe komplexným systémom. Jej prevádzka je reálne možná len na základe definovaných technických a organizačných opatrení pre rozširovanie, údržbu, realizáciu služieb, ale aj diagnostiku, riešenie problémov, monitorovanie stavu a optimalizáciu fungovania. Tieto opatrenia vychádzajú z legislatívy, štandardov a technickej praxe oboru. V práci boli na potrebnej úrovni detailnosti analyzované a diskutované.

Použitá literatúra

[1] ČESKÁ REPUBLIKA. *Ústava České republiky: ústavní zákon č. 1/1993 Sb. ve znění ústavního zákona č. 347/1997 Sb., 300/2000 Sb., 448/2001 Sb., 395/2001 Sb., 515/2002 Sb., 319/2009 Sb., 71/2012 Sb. a 98/2013 Sb*. In: . Praha: Česká národní rada, 16. prosince 1992n. l., ročník 1993, číslo 1. Dostupné také z: https://www.psp.cz/docs/laws/constitution.html

[2] SLOVENSKÁ REPUBLIKA. *Ústavný zákon č. 460/1992 Zb.: Ústava Slovenskej republiky*. In: . Bratislava: Slovenská národná rada, 1. septembra 1992n. l., ročník 1992, číslo 460. Dostupné také z: https://www.zakonypreludi.sk/zz/1992-460

[3] EU. SMERNICA RADY 2008/114/ES: *o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu*. In: *L 345/75*. ES: Úradný vestník Európskej únie, 2008, ročník 2008, číslo 114. Dostupné tiež z: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32008L0114&from=CS

[4] ČESKÁ REPUBLIKA. *Zákon č. 240/2000 Sb.: Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)*. In: . Česká republika: Parlament České republiky, 2000, ročník 2000, 73/2000, číslo 240. Dostupné tiež z: https://www.zakonyprolidi.cz/cs/2000-240

[5] ČESKÁ REPUBLIKA. *Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: . Česká republika: Parlament České republiky, 2014, ročník 2014, číslo 181. Dostupné tiež z: https://www.zakonyprolidi.cz/cs/2014-181

[6] 3GPP The Mobile Broadband Standard: Releases. *3GPP: A Global Initiative* [online]. 3GPP, 2020, 23.03.2020 [cit. 2020-05-11]. Dostupné z: https://www.3gpp.org/specifications/67-releases

[7] 3GPP The Mobile Broadband Standard: Mission Critical Services in 3GPP. *3GPP: A Global Initiative* [online]. 3GPP, 2017, 20.06.2017 [cit. 2020-05-11]. Dostupné z: https://www.3gpp.org/news-events/1875-mc_services

[8] 3GPP TS 22.280: Mission Critical Services Common Requirements (MCCoRe). *3rd Generation Partnership Project: Technical Specification* [online]. Technical Specification Group Services and System Aspects, 2016, 2016 [cit. 2020-05-11]. Dostupné z: https://www.3gpp.org/ftp/Specs/archive/22_series/22.280/

[9] HORST CZICHOS, editors. Handbook of technical diagnostics fundamentals and application to structures and systems. Berlin: Springer, 2013. ISBN 9783642258503.

[10] TICHÝ, Milík. *Ovládání rizika: analýza a management*. Praha: C. H. Beck, 2006. Beckova edice ekonomie. ISBN 80-717-9415-5.

[11] PROCHÁZKOVÁ, Dana, Vladimír ADAMEC, Jan PROCHÁZKA a Barbora SCHÜLLEROVÁ. *Terminologický slovník pro inženýrské disciplíny pracující s riziky v systémovém pojetí*. Brno: Akademické nakladatelství CERM, 2019, 68 s. ISBN 978-80-7623-000-2.

[12] JANÍČEK, Přemysl. *Systémová metodologie: Brána do řešení problémů*. Recenzenti: F. PEŠLOVÁ, J. MAREK. Brno: Akademické nakladatelství CERM, 2014. ISBN 978-80-7204-887-8.

[13] ČSN EN ISO 12100. *Bezpečnost strojních zařízení - Všeobecné zásady pro konstrukci - Posouzení rizika a snižování rizika*. Opr.1. Česká republika: Česká technická norma (ČSN), 2011. Bezpečnost strojních zařízení, 13.110.

[14] ŠENOVSKÝ, Michail, Vilém ADAMEC a Pavel ŠENOVSKÝ. *Ochrana kritické infrastruktury*. 51. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2007, 132 s. SPBI Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-025-8.

[15] KROČOVÁ, Šárka. *Bezpečnost provozu technické infrastruktury*. 94. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2017, 122 s. SPBI Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-185-9.

[16] PRCHAL, J. *Teorie pravděpodobnosti v sdělovací technice*. Vydání I. Praha: Nakladatelství dopravy a spojů, 1975. ISBN OS-31-022/76.

[17] *Circuit-switched fallback: The first phase of voice evolution for mobile LTE device.* QUALCOMM, Ericsson, 2012, 11 s.

[18] ZELINKA, Tomáš a Miroslav SVÍTEK. *Telekomunikační řešení pro informační systémy síťových odvětví*. 1. vyd. Praha: Grada, 2009, 218 s. Průvodce (Grada). ISBN 978-80-247-3232-9.

[19] ČSN EN IEC 60812. *Analýza způsobů a důsledků poruch (FMEA a FMECA)*. Ed. 2 (01 0675). Česká republika: Česká technická norma, 2019.

[20] ČSN EN 62502. *Techniky analýzy spolehlivosti: Analýza stromu událostí (ETA)*. 01 0676. Česká republika: Česká technická norma, 2011.

[21] ČSN EN 61025. *Analýza stromu poruchových stavů: FTA*. 01 0676. Česká republika: Česká technická norma, 2007.

[22] 3GPP TS 32.410; Telecommunication management; Key Performance Indicators (KPI) for UMTS and GSM. 16.0.0. 3GPP. http://www.3gpp.org/DynaReport/32410.htm

[23] 3GPP TS 32.450; Telecommunication management; Key Performance Indicators (KPI) for Evolved Universal Terrestrial Radio Access Network (E-UTRAN): Definitions. 16.0.0. 3GPP. http://www.3gpp.org/DynaReport/32450.htm

[24] 3GPP TS 32.451; Telecommunication management; Key Performance Indicators (KPI) for Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Requirements. 16.0.0. 3GPP. http://www.3gpp.org/DynaReport/32451.htm

[25] 3GPP TS 32.814; Telecommunication management; UTRAN and GERAN Key Performance Indicators (KPI). 7.0.0. 3GPP, 2017-06-07. http://www.3gpp.org/DynaReport/32814.htm

[26] 3GPP TS 32.454; Telecommunication management; Key Performance Indicators (KPI) for the IP Multimedia Subsystem (IMS); Definitions. 16.0.0. 3GPP. http://www.3gpp.org/DynaReport/32454.htm

[27] 3GPP TS 32.455; Telecommunication management; Key Performance Indicators (KPI) for the Evolved Packet Core (EPC); Definitions. 16.0.0. 3GPP. http://www.3gpp.org/DynaReport/32455.htm

[28] KREHER, Ralf. UMTS Performance measurement: a practical guide to KPIs for the UTRAN environment. Chichester: John Wiley, 2007, xii, 213 p. ISBN 04-700-3249-9.

[29] WALLS, Karla: How mobile usage changes when customers get 4G speeds. In: CIQUAL: Customer Insight [online]. 2012-11-05. Available from: http://www.ciqual.com/blog/how-mobile-usage-changes-when-customers-get-4g-speeds/

[30] *Digital News Report 2016*. Thomson Reuters Foundation. Oxford: Reuters Institute for the Study of Journalism, 2016, 124 s. Dostupné z: http://web.archive.org/web/20170207091856/https://reutersinstitute.politics.ox.ac.uk/news/digital-news-report-2016-out-now

[31] Český telekomunikační úřad: Výroční zpráva 2020. *ČTÚ* [online]. Český telekomunikační úřad, 2020, 94 s. [cit. 2021-6-7]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/stranky/382551/soubory/vzctu2020.pdf

Zoznam tabuliek

Zoznam obrázkov

Zoznam symbolov a skratiek

γ_x	pravdepodobnostná hranica pre parameter x
$\delta()$	binárna kriteriálna funkcia, vracajúca hodnotu 1 v prípade splnenia kriteriálnych podmienok, 0 v opačnom prípade
ε_x	prahová hodnota rozdielu medzi požadovanou a nameranou hodnotou parametra x
A	útlm
APN	vymedzujúce kritérium podľa cieľovej paketovo prepínanej siete pre analýzu používateľského dátového spojenia
avg()	funkcia vracajúca reálne číslo reprezentujúce aritmetický priemer hodnôt množiny zadanej ako parameter
B	byte – bajt, dátové slovo o veľkosti 8 bitov
base.time()	funkcia vracajúca reálne číslo reprezentujúce absolútny čas registrácie analyzovanej dátovej jednotky predanej ako parameter
C	súbor kritérií pre kriteriálnu funkciu $\delta()$
count()	funkcia vracajúca celočíselnú hodnotu reprezentujúcu počet spojení zodpovedajúcich konkrétnej zadanej podmienke
dB	jednotka výkonového či úrovňového rozdielu
$\text{Delay}_{\text{RAN}}$	oneskorenie v rádiovej prístupovej sieti mobilnej siete
d_i	požadovaná hodnota parametru pri vyhodnocovaní presnosti systému
$d_{m,i}$	nameraná hodnota parametru pri vyhodnocovaní presnosti systému
eth.tot_len()	funkcia vracajúca celkovú veľkosť dátovej jednotky na druhej vrstve (Ethernet rámec) predanej ako parameter
Element	vymedzujúce kritérium podľa obslužného prvku pre analýzu používateľského dátového spojenia
GL	vymedzujúce kritérium podľa geografickej lokality pre analýzu používateľského dátového spojenia
$\text{HTTP}_{\text{DTCR}}$	HTTP Data Transfer Corruption Ratio – pravdepodobnosť havárie HTTP relácie počas dátového prenosu
$\text{HTTP}_{\text{IPAT}}$	HTTP IP Access Time - doba prístupu k službe na nižšej vrstve v prípade HTTP relácie
$\text{HTTP}_{\text{IPAFR}}$	HTTP IP Access Failure Ratio - neúspešnosť nadviazania spojenia na nižšej vrstve v prípade HTTP relácie
HTTP_{SFR}	HTTP Service Failure Ratio – pravdepodobnosť zlyhania vytvorenia HTTP relácie
m	meter, základná jednotka vzdialenosti
N	celkový počet analyzovaných dátových jednotiek pre konkrétny KPI
P	výkon (vysielací)
$P(x)$	pravdepodobnostná funkcia, vracajúca pravdepodobnosť javu x
p_i	analyzovaná dátová jednotka pre konkrétny KPI, *i*-ta v poradí

pdp.all() funkcia vracajúca celočíselnú hodnotu reprezentujúcu počet všetkých realizovaných pokusov o aktiváciu kontextu paketovýc dát podľa vymedzujúcich kritérií zadaných ako parametre, v sledovanej dobe

PDP_{CAFR} PDP Context Activation Failure Ratio – neúspešnosť aktivácie kontextu protokolu paketových dát s danou požadovanou kvalitou služby

$PS_{Attach\ Time}$ Packet Switched Attach Time – doba nadviazania paketovo prepínaného spojenia, t.j. doba potrebná pre pripojenie používateľského koncového zariadenia k dátovej sieti pomocou paketovo prepínaného spojenia cez mobilnú sieť

q_i požadovaná hodnota parametru pri vyhodnocovaní dostupnosti systému

$q_{m,i}$ nameraná hodnota parametru pri vyhodnocovaní dostupnosti systému

Quality vymedzujúce kritérium podľa požadovanej kvality služby pre analýzu používateľského dátového spojenia

r polomer, vzdialenosť od bodu vysielania

r_i požadovaná hodnota parametru pri vyhodnocovaní kontinuity systému

$r_{m,i}$ nameraná hodnota parametru pri vyhodnocovaní kontinuity systému

s sekunda – základná jednotka času

S hustota energetického toku

S_r súhrnný počet relácií v používateľskej rovine v analyzovanom úseku

session analyzovaná relácia pre konkrétne KPI

s_i požadovaná hodnota parametru pri vyhodnocovaní integrity systému

$s_{m,i}$ nameraná hodnota parametru pri vyhodnocovaní integrity systému

T horná hranica časového intervalu $\langle 0, T \rangle$ pre vyhodnocovanie výkonových indikátorov

T_O celková priepustnosť spoja so započítaním transportnej réžie

UG vymedzujúce kritérium podľa zamerania na používateľa pre analýzu používateľského dátového spojenia

v_i požadovaná hodnota parametru pri vyhodnocovaní spoľahlivosti systému

$v_{m,i}$ nameraná hodnota parametru pri vyhodnocovaní spoľahlivosti systému

v_O celkový objem prenesených dát so započítaním transportnej réžie

v_U celkový objem prenesených dát bez započítania transportnej réžie (iba payload)

W_i požadovaná hodnota parametru pri vyhodnocovaní bezpečnosti systému

$W_{m,i}$ nameraná hodnota parametru pri vyhodnocovaní bezpečnosti systému

$HTTP_{SESSION\ TIME}$ doba trvania HTTP relácie

http.payload.size() funkcia vracajúca celočíselnú hodnotu reprezentujúcu celkové množstvo dát prenesené nad HTTP protokolom v danej relácii zadanej ako parameter

pdp.unsuccessful() funkcia vracajúca celočíselnú hodnotu reprezentujúcu počet neúspešne realizovaných pokusov o aktiváciu kontextu paketovýc dát podľa vymedzujúcich kritérií zadaných ako parametre, v sledovanej dobe

gtp.payload_len() funkcia vracajúca celočíselnú hodnotu reprezentujúcu veľkosť prenášaných dát protokolom GTP

$HTTP_{AVG\ SESSION\ TIME}$ priemerná doba trvania HTTP relácie za zledované obdobie

$HTTP_{AVG\ DATA\ RATE}$ priemerné množstvo dát prenesených protokolom HTTP na jednu reláciu za časové obdobie, väčšinou za hlavnú prevádzkovú hodinu

2G mobilná bunková sieť druhej generácie GSM

3,9G mobilná bunková sieť s rádiovou prístupovou sieťou LTE

3G mobilná bunková sieť tretej generácie UMTS

3GPP 3rd Generation Partnership Project – konzorcium spolupracujúce na špecifikácii mobilných sietí od tretej generácie ďalej

4G mobilná bunková sieť s rádiovou prístupovou sieťou LTE-Advanced

5G mobilná bunková sieť piatej generácie

7S metóda analýzy ekomických systémov zameraná na vnútorné prostredie podniku

A rozhranie mobilnej siete 2G medzi subsystémom základňových staníc BSS a subsystémom prepínania MSS, zabezpečujúce prenos dát používateľskej aj riadiacej roviny, slúžiace pre okruhovo prepínané služby

A-bis rozhranie subsystému základňových staníc mobilnej siete 2G medzi BTS a BSC pre prenos dát používateľskej aj riadiacej roviny

A-Netz historická technológia mobilnej siete prvej generácie s analógovým prenosom hlasu aj signalizácie, prevádzkovaná najmä v Nemecku

ACK TCP ACKnowledgement – príznak v hlavičke paketu protokolu TCP označujúci potvrdenie úspešného prijatia predchádzajúcich správ v opačnom smere

AMPS Advanced Mobile Phone System – historická technológia mobilnej siete prvej generácie s analógovým prenosom hlasu aj signalizácie vyvinutá a prevádzkovaná spoločnosťou AT&T

APN Access Point Name – názov prístupového bodu, používa sa pre rozlíšenie cieľovej externej paketovo komutovanej siete v mobilnom účastníckom koncovom zariadení

ARP Allocation and Retention Priority – parameter definujúci na úrovni riadiacej roviny mobilných sietí prioritu vytvorenia nosiča na úkor iných či jeho zrušenia v prípade vyčerpania kapacity

AT&T American Telephone and Telegraph – americká telekomunikačná spoločnosť

ATM Asynchronous Transfer Mode – technológia prenosu dát podporujúca zároveň režim prepínania dátových jednotiek a virtuálnych okruhov

B-Netz historická technológia mobilnej siete prvej generácie s analógovým prenosom hlasu aj signalizácie, prevádzkovaná najmä v nemecky hovoriacich krajinách Európy, zavádzajúca technológiu medzinárodného roamingu

Beidou systém pre určovanie polohy na zemeguli využívajúci príjem satelitného signálu a výpočtu polohy na základe vzdialenosti od jednotlivých satelitov so známou pozíciou, vybudovaný Čínskou ľudovou republikou, pôvodne označovaný ako COMPASS

BSC Base Station Controller – prvok riadiaci skupinu základňových staníc v mobilnej sieti GSM

BSS	Base Station Subsystem – subsystém mobilnej siete realizujúci rádiovú prístupovú sieť, pozostávajúci zo základňových staníc a ich riadiacich prvkov
BTS	Base Transceiver Station – základňová stanica v mobilnej sieti GSM
C-Netz	historická technológia mobilnej siete s analógovým prenosom hlasu aj signalizácie, prevádzkovaná najmä v nemecky hovoriacich krajinách Európy, podporujúca medzinárodný roaming a analógové šifrovanie hlasových dát
CDMA	Code Division Multiple Access – metóda zdieľania média založená na kódovom delení
CDMA2000	digitálna mobilná sieť tretej generácie založená na kódovom viacnásobnom prístupe, nekompatibilná s UMTS
CERT	Computer Emergency Response Team – tím pre reakciu na počítačovú núdzovú situáciu
CSD	Circuit Switched Data – systém prenosu dát cez okruhovo komutované spojenie v mobilnej sieti, podobné vytáčanému pripojeniu k dátovým sieťam (dial-up) z pevných telefónnych sietí
CSFB	Circuit Switched Fall Back – funkcia realizácie hovorovej služby v prípade využívania dátového spojenia v mobilnej sieti SAE kde chýba CS doména, hovorová služba sa realizuje v paralelne vybudovanej sieti 2G alebo 3G, ktorá CS doménu obsahuje
ČR	Česká republika
ČSN	Česká soustava norem – označenie českých technických noriem
ČTÚ	Český Telekomunikačný Úrad – autorita ČR pre správu kmitočtového spektra a ďalšie činnosti, napr. kontrolné, ohľadom elektronických telekomunikácií
DTT	Drive Test Tool – nástroj na meranie parametrov mobilných sietí metódou drive testing
E1	multiplexovaný systém prenosu s časovým delením do slotov používaný najmä v Európe
E2E	End to End – kvalifikátor označujúci že jav či proces sa aplikuje po celej trase, od jedného konca k druhému
ECI	European Critical Infrastructure - európska kritická infraštruktúra, teda kritická infraštruktúra európskeho (cezhraničného) významu
EDGE	Enhanced Data rates for GSM Evolution – systém paketového prenosu dát po rádiovom rozhraní mobilnej siete GSM, ktorý vznikol evolúciou systému GPRS
EN	Eurpean standards – sústava harmonizovaných technických noriem schvaľovaných Európskou radou, s okamžitou platnosťou bez zmien v členských krajinách EU, normy ISO sú podľa možností preberané pod EN bez zmien
EPC	Evolved Packet Core - jadro mobilnej siete 3,9G a 4G zabezpečujúce paketovo orientovaný prenos dát
ETA	Event Tree Analysis – analýza stromu udalostí, metóda analýzy rizika
ETSI	European Telecommunication Standards Institute - európsky inštitút pre telekomunikačné štandardy
EU	European Union – Európska únia
FMEA	Failure Mode and Effect Analysis – analýza spôsobov a dopadov porúch, metóda analýzy rizika
FTA	Fault Tree Analysis – analýza stromu porúch, metóda analýzy rizika
FTP	File Transfer Protocol - protokol pre prenos súborov z protokolovej sady TCP/IP

FUP	Fair Usage Policy – politika férového využívania služby, limit zavedený poskytovateľom pripojenia na parametre poskytovaného pripojenia, väčšinou vo forme maximálneho množstva prenesených dát za jednotku času, po vyčerpaní ktorého je služba obmedzená či dočasne deaktivovaná
Galileo	systém pre určovanie polohy na zemeguli využívajúci príjem satelitného signálu a výpočtu polohy na základe vzdialenosti od jednotlivých satelitov so známou pozíciou, vybudovaný Európskou vesmírnou agentúrou
Gb	rozhranie mobilnej siete 2G/3G medzi základňovou stanicou a prvkom SGSN, zabezpečujúce prenos dát používateľskej aj riadiacej roviny
GBR	Guaranteed Bit Rate – systém zabezpečenia kvality služby s vyhradením pásma pre konkrétnu službu či skupinu služieb
GGSN	Gateway GPRS Support Node - prvok mobilnej siete 2G a 3G zabezpečujúci funkcie smerovania komunikácie a rozhranie na externé dátové siete pri pripojení používateľského koncového zariadenia k paketovo prepínanej dátovej sieti
GLONASS	GLObal NAvigation Satellite System - systém pre určovanie polohy na zemeguli využívajúci príjem satelitného signálu a výpočtu polohy na základe vzdialenosti od jednotlivých satelitov so známou pozíciou, vybudovaný letectvom Ruskej federácie, s celosvetovým pokrytím a voľným použitím
Gn	rozhranie subsystému mobilnej siete GPRS medzi prvkami SGSN a GGSN zabezpečujúce prenos dát používateľskej roviny
GPRS	General Packet Radio Service – systém prenosu paketových dát po rádiovom rozhraní mobilnej siete GSM
GPS	Global Positioning System – systém pre určovanie polohy na zemeguli využívajúci príjem satelitného signálu a výpočtu polohy na základe vzdialenosti od jednotlivých satelitov so známou pozíciou, vybudovaný a prevádzkovaný orgánmi USA s medzinárodnou spoluprácou a možnosťou využitia entitami mimo USA
GSM	Global System for Mobile Communication – digitálna mobilná sieť druhej generácie s časovo oddeleným viacnásobným prístupom, podporujúca prenos hlasu, okruhovo spínaných dátových hovorov a krátkych textových správ SMS
GTP	GPRS Tunnelling Protocol – skupina protokolov používaných pre implementáciu prenosu paketovo prepínaných používateľských dát v mobilných sieťach GSM, UMTS či SAE/EPC
GTP-U	GPRS Tunnelling Protocol-User – podmnožina protokolu GTP, cielená na tunelovaný prenos používateľských dát paketovo prepínaným jadrom siete
HSDPA	High-Speed Downlink Packet Access - technológia pre siete UMTS zvyšujúca prenosovú kapacitu rádiového rozhrania v smere od základňovej stanice k mobilnému terminálu
HSPA	High Speed Packet Access – technológia pre siete UMTS zvyšujúca prenosovú kapacitu rádiového rozhrania, kombinujúca technológie HSDPA a HSUPA
HSUPA	High-Speed Uplink Packet Access – technológia pre siete UMTS zvyšujúca prenosovú kapacitu rádiového rozhrania v smere od mobilného terminálu k základňovej stanici
HTML	HyperText Markup Language – jazyk pre popis dokumentov s hypertextovými odkazmi

HTTP	Hypertext Transfer Protocol – protokol pre prenos HTML a ďalších dokumentov
IMS	IP Multimedia Subsystem – systém tvoriaci distribuovanú VoIP telefónnu ústredňu umožňujúci fixnú a mobilnú konvergenciu a realizáciu hovorových a iných služieb
IoT	Internet of Things – označenie pre dátové siete, kde komunikujúce strany nie sú účastnícke koncové zariadenia, a ich prostredníctvom používatelia, ale fyzické zariadenia a automatizované systémy
IP	Internet Protocol – protokol zabezpečujúci funkcie tretej vrstvy ISO/OSI, t.j. smerovania, v protokolovej sade TCP/IP
IS-136	Interim Standard-136 – historická technológia mobilnej siete druhej generácie s analógovým prenosom signalizácie a digitálnym kódovaním hlasových dát, evolúcia IS-54B, pridáva podporu CSD prenosov a prenos textových správ inšpirované systémom GSM
IS-54B	Interim Standard-54B – historická technológia mobilnej siete druhej generácie s analógovým prenosom signalizácie a digitálnym kódovaním hlasových dát, čiastočne kompatibilná evolúcia systému AMPS
IS-95 CDMA	Interim Standard-95 – historická technológia mobilnej siete druhej generácie založená na CDMA vyvinutá spoločnosťou Qualcomm
ISO	International Standardization Organization – štandardizačný orgán s medzinárodnou pôsobnosťou
KPI	Key Performance Indicators – kľúčový výkonnostný indikátor - súbor parametrov popisujúcich výkon nejakého zariadenia, systému alebo procesu
LTE	Long Term Evolution of UMTS – rádiová prístupová sieť mobilnej siete 3,9G, kompatibilná s jadrom mobilnej siete 4G
LTE-Advanced	rádiová prístupová sieť mobilnej siete 4G
M2M	Machine to Machine – sieťová komunikácia medzi dvoma zariadeniami neslúžiacimi ako účastnícke koncové zariadenia
MDTT	Morotola Drive Test Tool - nástroj na meranie parametrov mobilných sietí metódou drive testing od firmy Motorola
MIB	Management Information Base – stromová štruktúra definujúca systém informačných štruktúr o sieťovom zariadení používaná ako strom pri dohľadování a riadení protokolom SNMP
NMT	Nordic Mobile Telephone – historická technológia mobilnej siete prvej generácie s analógovým prenosom hlasu aj signalizácie, prevádzkovaná najmä v Európe a v častiach Ázie
OSP	Operator Security Plan, bezpečnostný plán prevádzkovateľa (kritickej infraštruktúry)
OTT	Over The Top – označenie služieb transportovaných infraštruktúrou bez hlbšej integrácie či prispôsobenia, služby pre ktoré je sieť využívaná ako prístupová
PDN	Packet Data Network – identifikátor paketového dátového spoja v SAE
PDP	Packet Data Protocol – protokol prenosu paketových používateľských dát v mobilných sieťach s prenosom založeným na prepínaní paketov GPRS

PERT	Program Evaluation and Review Technique – metóda pre hľadanie kritickej cesty prechodu orientovaným grafom súslednosti činností, používaná pri ekonomickej analýze procesov
QoS	Quality of Service – riadiaci a kontrolný mechanizmus rezervácie sieťových zdrojov so schopnosťou poskytovať rôzne úrovne priority rôznym dátovým tokom pre zaistenie vhodných vlastností prenosovej služby
RNC	Radio Network Controller - prvok riadiaci skupinu základňových staníc v mobilnej sieti UMTS
RTS	Real Time System – systém, pre ktorý je funkčne dôležité okrem formálnej správnosti výsledku aj jeho dodanie najneskôr v definovanom čase
RTT	Round Trip Time – doba odpovede vzdialeného systému pri komunikácii v sieti s prepínaním paketov myslená ako doba prenosu dátovou sieťou
S1	rozhranie mobilnej siete 4G medzi základňovou stanicou a prvkami EPC
S1	rozhranie mobilnej siete 4G medzi základňovou stanicou a prvkami EPC
S1-U	rozhranie mobilnej siete 4G medzi základňovou stanicou a prvkom SGW, služiace pre prenos dát používateľskej roviny
S1-U	rozhranie mobilnej siete 4G medzi základňovou stanicou a prvkom SGW, služiace pre prenos dát používateľskej roviny
S4	rozhranie mobilnej siete medzi prvkami 4G SGW a prvkami 2G/3G SGSN, zabezpečujúce interkomunikáciu paralelne vybudovaných sietí rôznych generácií, slúžiace pre prenos dát používateľskej aj riadiacej roviny
S5	rozhranie mobilnej siete 4G medzi prvkami jadra SGW a PGW v rámci siete jedného operátora, slúžiace pre prenos používateľských dát, v podstate identické s rozhraním S8
S8	rozhranie mobilnej siete 4G medzi prvkami jadra SGW a PGW v prípade roamingu, teda ak jednotlivé strany patria rôznym operátorom, slúžiace pre prenos používateľských dát, v podstate identické s rozhraním S5
SAE	System Architecture Evolution – označenie vývoja architektúry mobilnej siete 3,9G a 4G
SDF	Service Data Filter – logická konštrukcia identifikujúca a rozraďujúca jednotlivé služby v používateľskej rovine mobilných sietí s prenosom s komutáciou paketov
SGSN	Serving GPRS Support Node – prvok mobilnej siete 2G a 3G zabezpečujúci riadiace funkcie pri pripojení používateľského koncového zariadenia k paketovo prepínanej dátovej sieti
SGW	Serving GateWay – prvok EPC realizujúci funkcie prenosu a smerovania používateľských dát a napojenia EPC na 3GPP rádiovú prístupovú sieť
SIM	Subscriber Identity Module – modul identity účastníka
SIP	Session Initiation Protocol – signalizačný protokol pre službu IP telefónie VoIP
SLEPTE	analýza sociálnych, legislatívnych, ekonomických, politických, technologických a environmentálnych faktorov vonkajšieho prostredia podniku
SMS	Short Message Service – služba prenosu krátkych správ v mobilných sieťach druhej a tretej generácie

SNMP	Simple Network Management Protocol – protokol pre základnú správu a dohľadovanie zariadení sieťovej infraštruktúry v protokolovej rodine TCP/IP
SNR	Signal to Noise Ratio – (relatívny) odstup signálu od šumu
SPoF	Single Point of Failure – centrálne miesto zlyhania systému; bod, kde na rozdiel od zvyšku systému nie je zabezpečená redundancia v prípade poruchy
SR	Slovenská republika
SWOT	Strengths, Weaknesses, Opportunities, Threats – metóda analýzy rizík ekonomických systémov posudzujúca silné a slabé stránky podniku, príležitosti a hrozby vyplývajúce z jeho vnútornej štruktúry a konkurenčného prostredia
SYN	TCP SYNchronize - príznak v hlavičke paketu protokolu TCP označujúci žiadosť o nadviazanie spojenia
T1	multiplexovaný systém prenosu s časovým delením do slotov používaný najmä v USA
TACS	Total Access Communication System - historická technológia mobilnej siete prvej generácie, variant AMPS, využívaná najmä vo Veľkej Británii
TB	TeraByte – jednotka dátového objemu, 10^{12} bajtov
TCP	Transmission Control Protocol – protokol zabezpečujúci funkcie transportnej a relačnej vrstvy a poskytujúci spoľahlivú a spojovo orientovanú komunikačnú službu v protokolovej rodine TCP/IP
TCP/IP	množina komunikačných protokolov používaná v Internete a iných dátových sieťach, názov bol vytvorený zlúčením názvov dvoch najdôležitejších protokolov, TCP a IP
TETRA	TErrestrial Trunked RAdio – systém pre mobilnú komunikáciu a realizáciu sietí núdzových služieb pre použitie silovými a záchrannými zložkami
TFT	Traffic Flow Template – identifikátor konkrétneho toku v používateľskej rovine v mobilných sieťach
UMRA	Univerzálna matica rizikovej analýzy, metóda posúdenia rizika
UMTS	Universal Mobile Telecommunications System – digitálna mobilná sieť tretej generácie
URL	Universal Resource Locator – odkaz na zdroj vo webovej službe definujúci miesto uloženia tohto zdroja
URLLC	Ultra Reliable Low Latency Communication – technológia pre vysoko spoľahlivú komunikáciu s nízkym oneskorením v rádiovej sieti 5G mobilných sietí
USA	United States of America – Spojené štáty americké
VoLTE	Voice over LTE – technológia pre VoIP telefóniu kde aspoň jeden z účastníkov komunikácie je pripojený cez rádiovú prístupovú sieť LTE alebo LTE-Advanced
VPN	Virtual Private Network – technológia virtuálnej privátnej siete - pripojenie vzdialeného zariadenia k prostriedkom lokálnej počítačovej siete cez medziľahlú dátovú sieť
WiFi	Wireless Fidelity – technológia bezdrôtového prepojenia počítačov a sieťovej infraštruktúry
X2	rozhranie subsystému základňových staníc LTE a odvodených medzi dvoma základňovými stanicami, slúžiace pre prenos dát používateľskej aj riadiacej roviny, zabezpečujúce funkciu tzv. bezstratového handover-u používateľského terminálu

Zoznam príloh