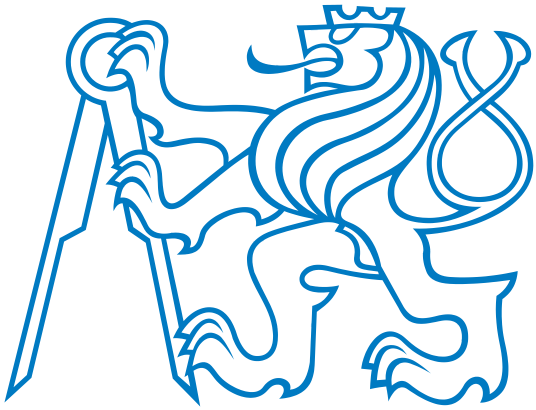


ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

DIPLOMOVÁ PRÁCE

Bc. Marek Oplištil

Návrh a ověření metodiky pro testování privátních sítí 5G využívaných v průmyslu

Fakulta elektrotechnická
Katedra telekomunikační techniky

Vedoucí diplomové práce: doc. Ing. Jiří Vodrážka, Ph.D.
Studijní program: Elektronika a komunikace
Specializace: Komunikační sítě a internet

Praha 2024

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé diplomové práce nebo její části se souhlasem katedry.

V Praze dne ....

Podpis autora

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Oplištil** Jméno: **Marek** Osobní číslo: **491829**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Elektronika a komunikace**

Specializace: **Komunikační sítě a internet**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Návrh a ověření metodiky pro testování privátních sítí 5G využívaných v průmyslu

Název diplomové práce anglicky:

Design and Validation of a Methodology for Testing 5G Private Networks Used in Industry

Pokyny pro vypracování:

Zpracujte analýzu vlastností sítí 5G, zejména z pohledu využití v průmyslu (sítě SA, kampusové sítě, podpora Industry 4.0). Navrhněte metodiku pro jejich testování pomocí platformy F-Tester, včetně vícebodových zátěžových testů, ověřování parametrů QoS, ověřování SLA. Zpracujte doporučení pro rozšiřování pokrytí a případnou diferenciaci služeb v průmyslových areálech.

Seznam doporučené literatury:

[1] Pobořil Vít - Testování sítí 5G pro obecné použití a aplikace v průmyslu a energetice, bakalářská práce, ČVUT v Praze, 2022
[2] Dokumentace k zařízení F-Tester - měření datových sítí dostupná na https://f-tester.fel.cvut.cz [on-line]

Jméno a pracoviště vedoucí(ho) diplomové práce:

doc. Ing. Jiří Vodrážka, Ph.D. katedra telekomunikační techniky FEL

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

Datum zadání diplomové práce: **01.02.2024** Termín odevzdání diplomové práce: **24.05.2024**

Platnost zadání diplomové práce: **21.09.2025**

doc. Ing. Jiří Vodrážka, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Mgr. Petr Páta, Ph.D. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

. | Datum převzetí zadání

Podpis studenta

Poděkování

Mé poděkování patří panu doc. Ing. Jiřímu Vodrážkovi, Ph.D. za odborné vedení práce, nepostradatelné rady, věcné připomínky, ochotu a za zapůjčení testovacích zařízení. Dále děkuji panu Ing. Zbyňku Kocurovi, Ph.D. za cenné rady a pomoc při nastavování testovacích zařízení F-Tester. Také děkuji panu Ing. Jakubu Hamerníkovi, MBA. za poskytnuté informace a možnost testovat privátní síť 5G ve výrobní hale společnosti *Continental Automotive*. Rovněž bych rád poděkoval za podporu při psaní diplomové práce své rodině.

Abstrakt

Testování síťových parametrů privátních sítí 5G je klíčové pro ověřování stavu sítě a kvality služby, což je důležité především pro provozování kritických aplikacích, kde jejich výpadek může mít neblahé následky. Tato diplomová práce je věnována privátním sítím 5G využívaných v *Průmyslu 4.0* a návrhu metodiky pro jejich testování pomocí platformy F-Tester založenou na dokumentu RFC 6349. Metodika popisuje postupy pro zjištění síťových parametrů a chování sítě pro případy, mezi které se řadí testování maximální propustnosti sítě, testování konkurence mezi TCP a UDP toky v síti pomocí vícebodových zátěžových testů, zatěžování sítě konstantními či proměnnými UDP toky a emulování určitého síťového provozu, kterému může být síť běžně v průmyslu vystavována. Navržená metodika je využitelná hlavně pro výkonnostní testování privátních sítí 5G. Ověření této metodiky proběhlo ve společnosti *Continental Automotive*, která implementuje privátní síť 5G. Jednotlivé testovací scénáře pomocí platformy F-Tester proběhly ve stacionárních bodech a za pohybu. Jsou uvedeny naměřené veličiny v čase jako je propustnost sítě, zpoždění ve smyčce, ztrátovost paketů i signálové parametry a zjištěné jevy jsou diskutovány. Dále bylo zpracováno doporučení pro rozšiřování pokrytí signálem a diferenciaci služeb v průmyslových areálech.

Klíčová slova: privátní sítě 5G, Průmysl 4.0, F-Tester, testování síťových parametrů, TCP, FlowPing, QoS

Abstract

Testing the network parameters of private 5G networks is crucial for verifying the network status and quality of service, which is especially important for running critical applications where their failure can have fatal consequences. This diploma thesis deals with private 5G networks used in *Industry 4.0* and the design of a methodology for testing them using the F-Tester platform based on RFC 6349. The methodology describes procedures for determining network parameters and network behaviour for cases that include testing the maximum network throughput, testing competition between TCP and UDP flows in a network using multi-point stress tests, overloading networks with constant or variable UDP flows, and emulating certain network traffic that a network may be exposed to in the industry. The proposed methodology is mainly usable for performance testing of private 5G networks. The validation of this methodology took place at company *Continental Automotive* which implements a private 5G network. Testing scenarios were performed with stationary and moving F-Testers. Measured network parameters over time, such as network throughput, latency, packet loss rate and signal parameters, are illustrated in figures and the found phenomena are discussed. Next, recommendations for signal coverage expansion and service differentiation in industrial campuses were suggested.

Keywords: private 5G networks, Industry 4.0, F-Tester, testing of network parameters, TCP, FlowPing, QoS

Obsah

Úvod

Tato diplomová práce se zabývá privátními sítěmi 5G z pohledu využití v průmyslu. Dokument *Analýza českého průmyslu 2024* [1] vydaný *Národním centrem Průmyslu 4.0* popisuje úroveň digitální zralosti firem v České republice. Z něj vyplývá, že digitalizace může přispět firmám k vyšší výrobní efektivitě, sběru dat, produktivitě, optimalizacím logistických tras a konkurenceschopnosti. Hlavní motivací firem k tomu, aby se digitalizací zabývaly a implementovaly daná řešení je efektivita lidí a zkrácení času, který je potřeba k uvedení nového produktu na trh, a to bez ztráty kvality.

Digitalizace je důsledkem nárůstu síťového provozu, který souvisí s obsluhou vysokého počtu senzorů a dalších zařízení v rámci továrny i jejího okolí. S tím rostou i nároky na síťovou infrastrukturu využívanou v průmyslu. Mezi typické požadavky na komunikační infrastrukturu se řadí vysoká přenosová rychlost, nízké zpoždění při přenosu a nízká ztrátovost paketů. Vhodná je například privátní sít 5G, která disponuje těmito vlastnostmi. Cílem této diplomové práce je analyzovat vlastnosti sítí 5G především z pohledu využití v průmyslu, navrhnout metodiku pro jejich testování pomocí platformy F-Tester a zpracovat doporučení pro rozšiřování pokrytí a diferenciaci služeb v průmyslových areálech.

Diplomová práce je rozdělena do šesti kapitol. Kapitola 1 je zaměřena na koncept *Průmysl 4.0* a důležitost dat, která mohou být následně využita pro umělou inteligenci a strojové učení. Kapitola je uzavřena popisem současné situace v českém průmyslu. Analýzou sítí 5G se zabývá kapitola 2 a část této kapitoly je věnována popisu využití sítí 5G v průmyslu. Kapitola 3 nastiňuje problematiku QoS a diferenciace služeb v komunikačních sítích.

Kapitola 4 je zaměřena na testování sítí na transportní vrstvě pomocí protokolů TCP a UDP. Na základě této kapitoly a dokumentu RFC 6349 [2] je navržena metodika pro testování privátních sítí 5G pomocí platformy F-Tester, kterou obsahuje kapitola 5. Kapitola 6 popisuje ověření této metodiky na privátní síti 5G společnosti *Continental Automotive* v Brandýse nad Labem. Obsahuje vyhodnocení dosažených výsledků i doporučení pro rozšiřování pokrytí signálem a diferenciaci využívaných služeb v síti.

1. Průmysl 4.0

Hlavní myšlenkou konceptu *Průmysl 4.0* (Industry 4.0) je propojení výrobních strojů, produktů a všech systémů průmyslového podniku. Cílem je vytvořit inteligentní distribuovanou síť různorodých entit a subsystémů, které pracují relativně autonomně a navzájem komunikují podle potřeby [4]. Dochází ke spojení virtuálního světa s fyzickým, kde části fyzického světa budou disponovat vysokorychlostním připojením se svou individuální IP (Internet Protocol) adresou, což je princip IoT (Internet of Things). Softwarové moduly představují fyzické prvky ve virtuálním prostoru [5]. Hlavní rysy konceptu *Průmysl 4.0* jsou [6]:

- digitalizace,
- automatizace,
- senzory a aktuátory,
- autonomní roboti,
- transformace výrobních procesů,
- kyberneticko-fyzické systémy,
- komunikační infrastruktura,
- datová úložiště a cloudové výpočty,
- kybernetika a umělá inteligence,
- big data,
- internet věcí,
- multiagentní systémy,
- aditivní výroba,
- rozšířená realita,
- virtualizace a simulace.

Pro zvyšující se požadavky na procesy je vhodné mít připravenou komunikační infrastrukturu. Automatizace je důsledkem nárůstu komunikace, která souvisí s obsluhou vysokého počtu senzorů a dalších zařízení. Mezi typické požadavky na komunikační infrastrukturu se řadí vysoká přenosová rychlost, nízké zpoždění při přenosu a spolehlivost. Vhodná je například 5G Standalone síť (viz kapitola 2), která má dle potřeby nastavené vlastní jádro a hardware [5].

Pro optimalizaci logistických procesů je užitečné mít informace o poloze objektů na úrovni jednotlivých továren, budov, komplexů nebo i na úrovni regionů. Důležité to je pro sledování a řízení pohybu materiálu nebo zboží. Digitální vozík může vyjet ven z haly a neztratí konektivitu například díky 5G Standalone síti,

která dokáže zajistit pokrytí továrny i jejího okolí. Využití této geolokace (zjištění polohy objektů) nahradí instalaci RTL (Real Time Location) systému, který využívá tagy RFID (Radio Frequency Identification).

Pro *Průmysl 4.0* je klíčový sběr a vyhodnocení dat z různých zdrojů, mezi které se řadí firemní informační systémy nebo data z výrobních strojů. Významný pojem je *big data*, který zahrnuje kombinaci strukturovaných, polostrukturovaných a nestrukturovaných dat. Zahrnuta jsou především textová, obrazová, obchodní, bezpečnostní a naměřená data. Pojem *big data* je charakterizován velkým objem různorodých dat z různých prostředí a rychlostí generování, shromažďování a zpracovávání dat. Objem dat se pohybuje v řádech terabajtů, petabajtů a dokonce i exabajtů dat, který se vytvořil a shromáždil v průběhu času [7].

1.1 Využití datové vědy v průmyslu

Datová věda se zabývá sběrem, přípravou a analýzou dat. Získání dat a práce s nimi je o tom usnadnit různé procesy ve firmě a o definování, zejména na začátku, k čemu by data mohla sloužit a jakou informaci z nich lze získat. Datová věda poskytuje pro výrobní firmy [8]:

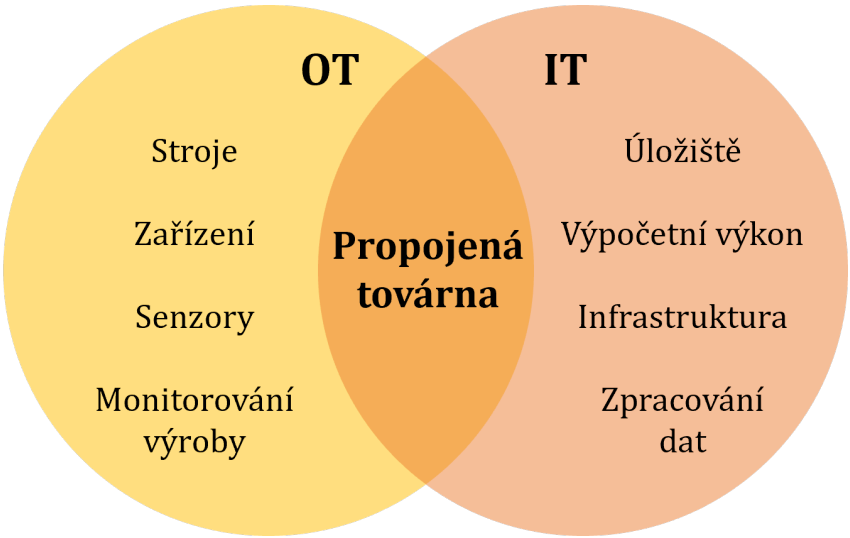
- rozhodování,
- predikování,
- integraci dat,
- správné třídění dat,
- řízení firmy efektivně jako celek,
- snížení chybovosti ve výrobním procesu,
- zapojení umělé inteligence a strojového učení,
- ekonomické úspory,
- vylepšování produktů,
- spokojenost zákazníků.

Integrace dat je vzájemné propojování dat získaných z různých systémů. Pokud jsou posuzována jednotlivá data separátně, tak je nelze hodnotit ve vzájemném kontextu. Když jsou data integrována a porovnávána v rámci firmy, tak lze vytvořit úspory, řítit firmu efektivně jako jeden celek, plánovat a předvídat různé situace. Například integrace dat umožňuje operátorům výrobní firmy rozhodování na základě dat, nikoliv na základě toho, co si myslí. Také nemusejí obcházet firemní oddělení nebo továrny s tužkou a papírem, aby si připravili vstupy pro další rozhodnutí či firemní porady. Dále reprezentace dat pomocí virtuální reality může usnadnit práci pracovníkům. Virtuální realita rozšiřuje lidské vnímání světa pomocí brýlí. Předává vizuální informace v podobě textových popisků a obrázků, které jsou umístěny někde v zorném poli pracovníka nebo jsou přímo umístěny do prostoru pozorovaných objektů.

Manažerům integrace dat zajišťuje to, že když přijdou do firmy, tak mohou mít okamžitý přehled o situaci ve firmě, což jim usnadní jejich rozhodování. Uvidí přehled celé firmy v jedné aplikaci a usoudí, co je správně nebo špatně. Dále, aby se předešlo neshodám na firemních poradách o tom, kdo má správná data, je vhodné mít jeden zdroj dat (Data Warehouse). Z jednoho zdroje dat lze udělat analýzu, vidět reporting, tvořit predikce nebo využít umělou inteligenci. Zároveň lze uložená data snadno sdílet, a tím bude firma transparentní. Tak vzniká možnost sdílet data s ostatními firmami, které vstupují do procesu, jako jsou například dodavatelé, a těžit ze získaných dat uložených na jednom místě. Ideální je prezentovat tyto údaje online a také brát v potaz bezpečností riziko, které tato transparentnost může přinést.

Typický model ve firmách je, že máme stranu OT (Operational Technology, výrobní část) a IT (Information Technology). Tyto dvě části jsou často oddělené a nekomunikují spolu. Proto je vhodné je propojit a získat tak mnoho možností, jak využít data z OT v IT (viz obrázek 1.1). Zároveň je nutné mít připravenou komunikační infrastrukturu, jako je například 5G Standalone síť (viz kapitola 2), která má dle potřeby nastavené vlastní jádro a hardware.

Dalším příkladem využití datové vědy je prediktivní údržba. Předvídáním se minimalizují výpadky, optimalizuje se plánování a prodlužuje se životnost zařízení. Pokud mám k dispozici data nasbíraná přímo z výroby, tak lze zabránit poruchám nebo odstávkám výroby. Například pro firmy z automobilového průmyslu může výpadek produkce znamenat vysoké pokuty.



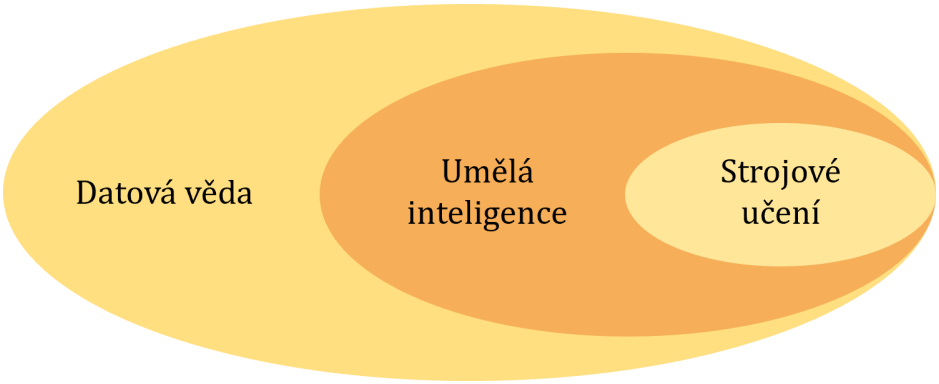
Obrázek 1.1: Integrace OT a IT.

1.2 Využití umělé inteligence a strojového učení v průmyslu

Datová věda spolu s umělou inteligencí a strojovým učením jsou nepostradatelnými prvky pro *Průmysl 4.0*. Datová věda je nezbytná pro umělou inteligenci a strojové učení. Umělá inteligence (AI – Artificial Intelligence) je soubor softwarových nebo hardwarových technologií. Pomáhá automatizovat, zrychlovat, zpřesňovat nebo škálovat lidské kognitivní schopnosti, mezi které se například řadí rozeznávání okolí, analyzování zvuku, porozumění řeči, zpracování informací, generalizování informací, dedukování další faktů a rozhodování dle vypozorovaných nebo vypočítaných dat [9].

Škálování kognitivních schopností umožní vysokou efektivitu například při analyzování fotografií nebo videí. Pomocí umělé inteligence se zhlédne například milión fotografií a určí se, jestli je na fotografiích například tygr či něco jiného. Člověk takové množství fotografií za stejný čas posoudit nedokáže. Umělá inteligence tedy umožňuje strojům nebo systémům chápat, uvažovat, interpretovat, učit se, učinit rozhodnutí a přizpůsobovat se [9].

Strojové učení (ML – Machine Learning) je podmnožinou datové vědy a umělé inteligence (viz obrázek 1.2). Zahrnuje algoritmy, které pomáhají s vylepšením strojů pod dohledem nebo bez dohledu. Jedná se o aplikovanou statistiku, kde jsou základním předpokladem trénovací a testovací data. Na trénovacích datech se vyladí model strojového učení. Tím se ukáže, jak vypadá vstup a očekávaný výstup. Natrénuje se tak, aby měl uspokojivé výsledky a pak se model testuje na testovacích datech, která jsou odlišná od trénovacích dat. Tím se ověřuje, jestli model funguje. Pokud ne, tak se dále upravují parametry, aby se výsledky blížily očekávaným výstupům. Například se zjistí, že model funguje s 85% pravděpodobností [9].



Obrázek 1.2: Vazba datové vědy, umělé inteligence a strojového učení.

Čím více je k dispozici dat, tím kvalitnější daný model je. Nejčastějším příkladem modelu jsou neuronové sítě. Model má vstup a vypočítá nějaký výstup. Například na vstupu může být obrázek, řečová nahrávka nebo zadání napsat článek a na výstupu tak bude kategorie zobrazeného objektu, transkript nebo článek.

Potenciál umělé inteligence pro *Průmysl 4.0* může mít do budoucna přínos v tom, že na základě zadání dokáže vygenerovat co nejlepší řešení pro určitý případ. Standardní automatizace je založená na očekávatelné opakovatelnosti, což

znamená, že roboti pracují s předměty, o kterých se již ví, kde jsou, jak vypadají a jak se má s nimi naložit. V případě umělé inteligence se očekává, že nastane stav, kdy se dosáhne automatizace i pro nestrukturované projekty, respektive jejich strukturovanost by byla menší než v současnosti.

Umělá inteligence má přínos i pro bezpečnost člověka a stroje. Může řídit autentizaci i autorizaci technologií, zaznamenávat kdo a kde co udělal a zpracovávat obrazová data (pro strojové učení). Může mít využití pro detekci a klasifikaci různých druhů překážek, plánování trajektorie a inteligentní kooperace s člověkem. Například autonomní roboti musí reagovat na situace, se kterými se při experimentech nepočítalo, a také musí sami vyřešit, jak se vyhnout atypickým překážkám, tedy přizpůsobit se situacím, na které nebyli trénovaní. Díky umělé inteligenci jsou schopni se autonomně pohybovat, samostatně plánovat trajektorie, vykreslit mapy (geolokace v reálném čase) a přizpůsobovat se prostředí.

Autonomní roboty lze například vybavit senzorikou na sledování teploty, vlhkosti a čistoty ovzduší. Mohou sloužit pro inspekční účely v průmyslovém prostředí a mohou poskytnout zpětnou vazbu, která se využije ve virtuální realitě a vytvoří dojem, jako by byl operátor na místě robota. Vhodné je, aby autonomní roboti komunikovali přes síť 5G Standalone kvůli vlastnostem této sítě (viz kapitola 2).

1.3 Situace v českém průmyslu

Situaci v českém průmyslu popisují analýzy vypracované *Národním centrem Průmyslu 4.0* [1, 3], které vznikly ve spolupráci s výrobními firmami. V roce 2023 tyto firmy uvedly, že mají především nedostatek kvalifikovaných pracovních sil. Dále je brzdila vysoká míra inflace a s tím i vysoká míra peněz, která firmám znepřístupňovala investiční úvěry potřebné pro jejich rozvoj. Také byly problémy s dodávkami oceli a elektrotechnických komponent.

Česká ekonomika je charakteristická tím, že růst mezd se vždy zvyšoval více než růst produktivity práce a dlouhá léta to bylo přibližně dvojnásobně, v roce 2023 to bylo čtyřnásobně. Z toho plyne, že firmy potřebují zvyšovat efektivitu své práce. Z konvenčních způsobů se firmy většinou vyčerpaly, avšak datová věda může zvýšit efektivitu práce. Správná interpretace dat může za relativně malé finanční prostředky výrazně přispět k vyšší produktivitě a k celkovému fungování výrobních firem [3].

V praxi dělají výrobní firmy řadu chyb. Naprostá většina firem nějaká data sbírá, ale pak je problém zejména integrace získaných dat, správné třídění, vyhodnocení a často se sbírají neúplná nebo nepřesná data, což může vést k chybným závěrům. Některé firmy nemají aktuální data, zveřejňují je v intervalech od jednoho dne až po měsíce [3].

Hlavní motivací firem k tomu, aby se digitalizací zabývaly a implementovaly daná řešení je efektivita lidí a rychlost uvedení na trh. Například pro strojírenství je především důležité zvýšit flexibilitu výroby, kvalitu výroby a dohledatelnost výrobku. Automobilový průmysl vede v digitalizaci dodavatelsko-odběratelských řetězců, logistiky, kontroly kvality a důrazu na rozvoj zaměstnanců [1].

Svaz průmyslu a dopravy České republiky vypracoval průzkum [10], který monitoruje, co se v prostředí implementace konceptu *Průmysl 4.0* odehrává. Celkem 98 průmyslových firem bylo zahrnuto pro sběr dat v roce 2023 v srpnu. Spektrum

respondentů pokrývalo hlavní odvětví české ekonomiky. Téměř 60 % firem má definovanou strategii pro digitální transformaci firmy. Firmy od digitální transformace nejčastěji očekávají [10, 11]:

- zlepšení tržní pozice ve vztahu ke konkurenci, což zahrnuje efektivní výrobu, optimalizaci uplatňování jejich prvků na trhu a lepší výběr dodavatelů v rámci otevření se nějakému digitálnímu okolí,
- větší odolnost vůči krizím a recesím, tedy rychlejší reakci na aktuální dění kolem sebe a přizpůsobivost obchodní i výrobní strategie,
- zachování současné pozice na trhu, další možné dopady digitalizace jsou očekávány později.

Nejčastější cíle firem v oblasti digitální transformace, které chtějí dosáhnout v příštích letech jsou [10, 11]:

- zvýšení produktivity,
- zlepšení kybernetické bezpečnosti,
- modernizace IT struktury.

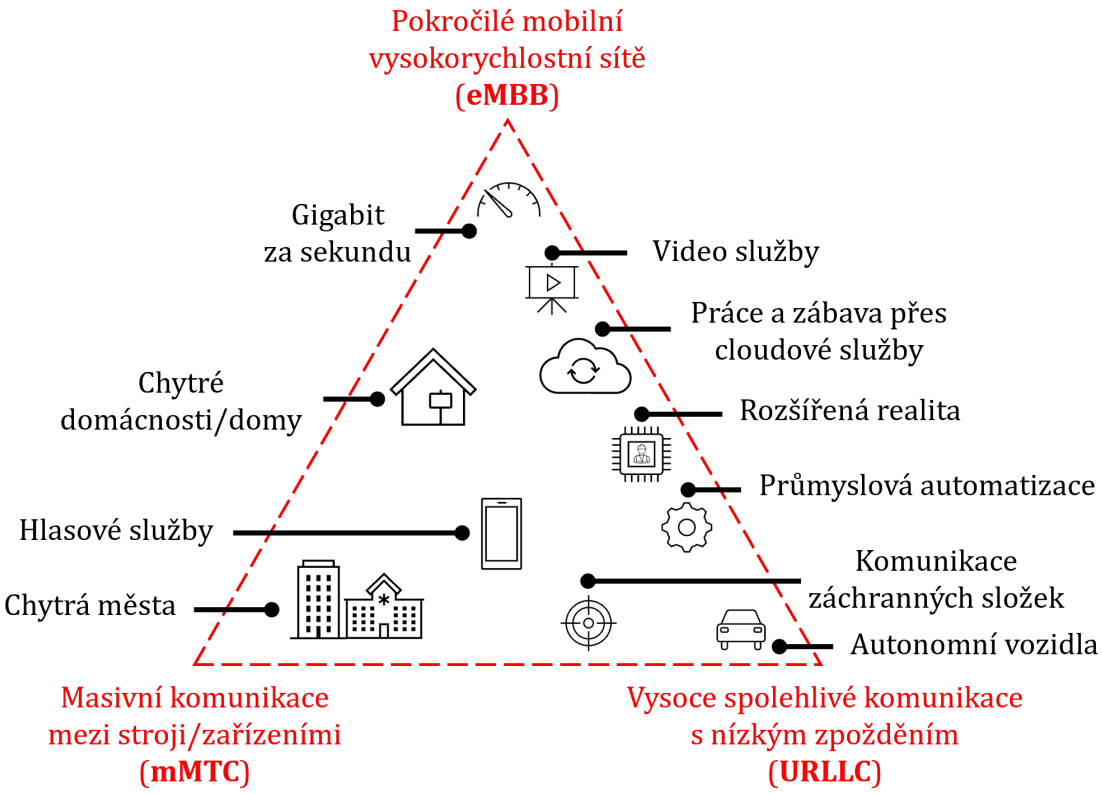
Mezi trendy vysledované za posledních 5 let patří [11]:

- implementace prvků *Průmyslu 4.0*, která se posouvá, avšak pomalu,
- rostoucí podíl firem se zpracovanou strategií pro digitální transformaci,
- trvající motivy pro investice do prvků *Průmyslu 4.0*, mezi které se řadí poskytování nových služeb, zrychlení vývoje a uvádění nových výrobků na trh,
- téma kybernetické bezpečnosti, které rezonuje a vzrostl podíl firem, které investovaly do vylepšení zabezpečení firemních dat,
- rostoucí podíl firem, které nasazují prvky *Průmyslu 4.0* v oblasti administrativních činností,
- problém v nasazování nových technologií, kde je častou překážkou nedostatek kvalifikovaných pracovníků.

2. Sítě 5G

Na vývoj sítí 5G působí organizace 3GPP (3rd Generation Partnership Project) a ITU (International Telecommunication Union). ITU stanoví doporučené postupy a 3GPP vytvoří technické standardy [12]. Obrázek 2.1 zobrazuje trojúhelník, který obsahuje oblasti pro nasazení sítí 5G. V jeho rozích jsou tři zásadní vlastnosti, a to vysokorychlostní přenos dat, nízké zpoždění a možnost připojit velký počet zařízení na km^2. Nedosáhne se všech těchto vlastností zároveň, kombinují se dle požadovaných služeb. Tyto vlastnosti jsou definovány ITU jako [12]:

- **eMBB** – enhance Mobile Broadband (pokročilé mobilní vysokorychlostní sítě),
- **URLLC** – Ultra Reliable and Low Latency (vysoce spolehlivé komunikace s nízkým zpožděním),
- **mMTC** – Massive Machine Type Communication (masivní komunikace mezi stroji či zařízeními).

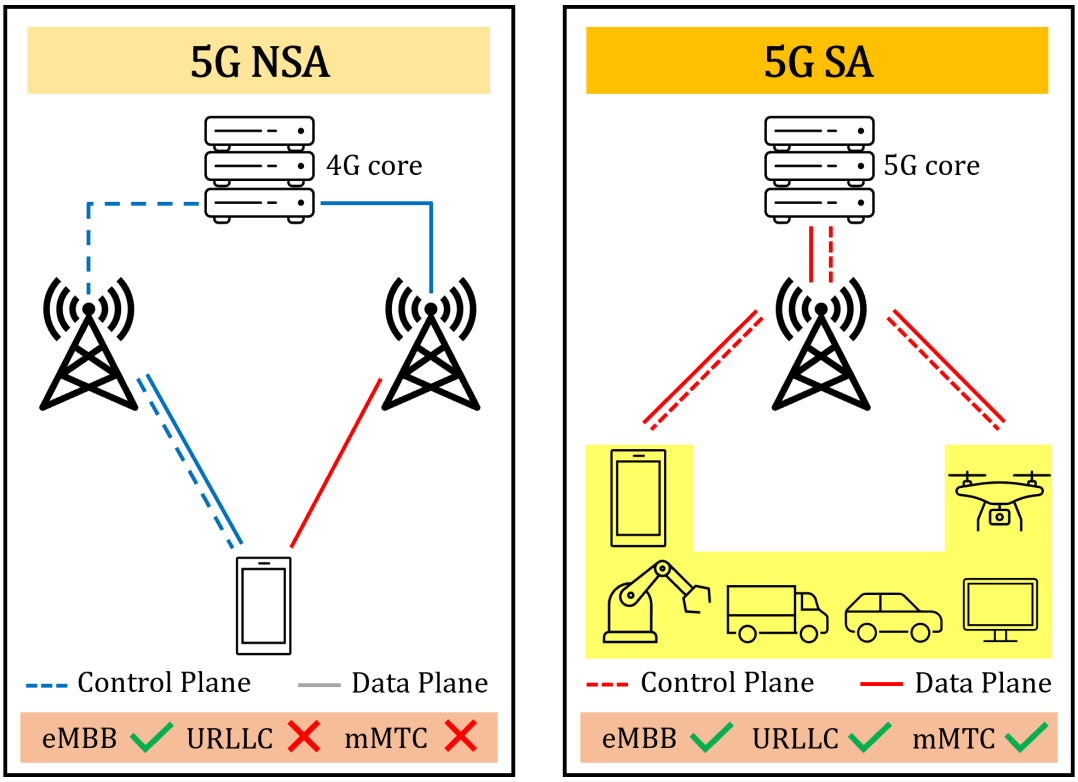


Obrázek 2.1: Oblasti nasazení sítí 5G [5].

Atribut **eMBB** zajišťuje vysoké přenosové rychlosti a vyšší mobilitu. Poskytuje přenosovou rychlost až desítky Gbit/s a mobilita je přibližně 500 km/h (vhodné pro vysokorychlostní železnice). Je nepostradatelný pro streamování videí ve vysokém rozlišení a pro virtuální realitu. Atribut **URLLC** přináší spolehlivost a nízké zpoždění (až 5 ms v jednom směru přenosu). Spolehlivost 99,999 % je pro přenosové rychlosti 50 kbit/s až 10 Mbit/s. Aplikace a zařízení vyžadující

nízké zpoždění jsou například komunikace v silniční dopravě, robotické operace, řízení dronů či monitorování výroby. Atribut **mMTC** poskytuje propojení velkého množství zařízení k síti 5G v určité oblasti, a to až milion zařízení na 1 km^2 s přenosovou rychlostí 1 až 100 kbit/s na jedno zařízení. Jedná se o významný atribut pro továrny s vysokou hustotou výrobních strojů, senzorů a aktuátorů [5].

Síť 5G má dvě etapy (viz obrázek 2.2). První etapa zahrnuje nesamostatný režim NSA (Non-Standalone), tedy 5G koexistuje s mobilní sítí 4G. Je využito technologie 5G NR (New Radio), která je podřízená 4G technologii, což zajišťuje pouze vyšší přenosovou rychlost (eMBB), ale ne zbylé dva klíčové atributy sítě 5G [13].



Obrázek 2.2: Rozdíly ve struktuře sítí 5G NSA a 5G SA [15].

Druhá etapa je samostatný režim SA (Standalone), která již není závislá na síti 4G pro signalizaci a datový přenos. Základnová stanice 5G je připojena pouze do jádra sítě 5G. Síť 5G SA již díky jádru sítě 5G umožňuje, kromě vysoké přenosové rychlosti, také nízké zpoždění a propojení velkého množství zařízení k síti, zatímco síť 5G NSA je především charakterizována vysokou přenosovou rychlostí [13]. Tedy mezi hlavní jevy, které síť 5G SA umožňuje, se řadí [14]:

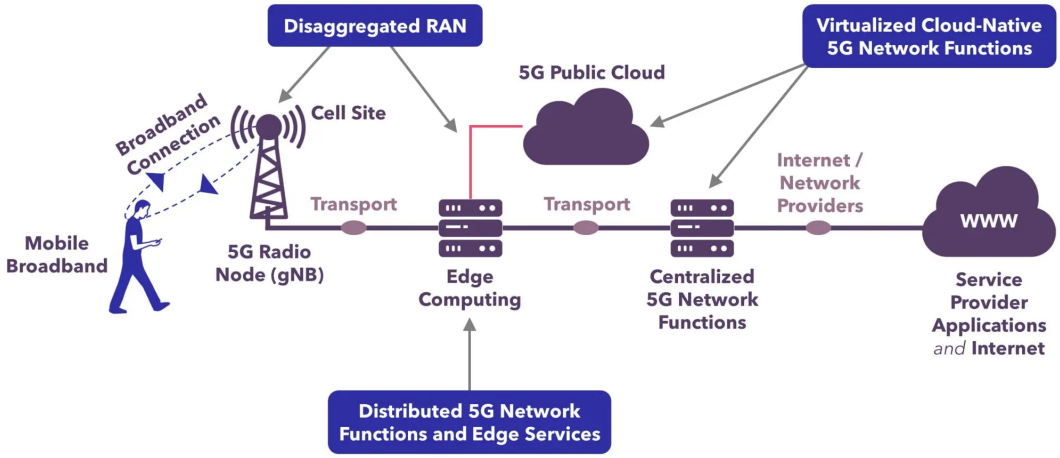
- nízké zpoždění při přenosu (garance až 5 ms),
- možnost připojení vysokého počtu zařízení (až milion zařízení na 1 km^2),
- vysoká přenosová rychlost (až 10 Gbit/s),
- stabilita, která je garantována a její dostupnost lze využívat pro kritické procesy (například zabezpečení lidí na pracovišti),

- bezpečnost (všechna komunikace je šifrována a nikdo neautorizovaný se nemůže připojit),
- tvorba privátních sítí 5G (kampusových sítí),
- network slicing a edge computing.

2.1 Architektura a jádro sítí 5G SA

Obrázek 2.3 zobrazuje architekturu sítě 5G SA. Základem je jádro sítě 5G (Core Network) a rádiová přístupová síť (RAN – Radio Access Network). Základnová stanice 5G (gNB – Next Generation Node B) je již připojena pouze do jádra sítě 5G, které zajišťuje především autentizaci, autorizaci, zabezpečení, mobility management, správu relací a agregaci provozu z připojených zařízení [16]. Toto jádro je softwarová záležitost a je založeno na principu nativního cloudu, což umožňuje tvořit škálovatelné aplikace v dynamických prostředích, mezi které patří veřejné, privátní a hybridní cloudy [17].

Bez cloudu by nemohl existovat edge computing, který umožňuje přiblížení výpočetních zdrojů k místu, ve kterých jsou data generována. Tak lze spouštět aplikace a zpracovávat data blízko koncovému zařízení, tedy přenést výpočetní kapacitu na „hranu“ sítě. To umožní snížení zpoždění při přenosu, zrychlení procesů a zajištění analýzy dat umožňující rychlou dostupnost k aktuálním výsledkům. Edge computing je důležitý například pro inteligentní výrobní systémy v továrnách, kde zařízení musí zpracovávat data z různých senzorů v reálném čase [18].



Obrázek 2.3: Architektura sítě 5G SA [18].

Jádro sítě 5G podporuje network slicing, což umožňuje tvorbu virtuálních vrstev, které jsou různě nastaveny dle potřeby pro nějaké služby [18]. Například jedna vrstva je optimalizována pro služby, které vyžadují nízké zpoždění při přenosu, druhá pro vysokou přenosovou rychlost a třetí pro vysoký počet zařízení. Sítě 5G SA jsou flexibilní a umožňují tak vytvořit síť dle požadavků zákazníka.

Je vhodné zajistit konektivitu základnových stanic 5G pomocí optických vláken (backhaul), aby nevzniklo tzv. *úzké hrdlo* a nedošlo tak k omezení vlastností sítí 5G. Mezi hlavní výhody optických vláken se řadí velká šířka pásma (200 THz), malý útlum (0,2 až 0,3 dB/km), odolnost proti elektromagnetickému záření, bezpečnost přenosu a vysoká systémová spolehlivost [19].

2.2 Kmitočtová pásma sítí 5G

Pro mobilní sítě 5G byla v Evropě stanovena tři kmitočtová pásma 700 MHz, 3,4–3,8 GHz a 26 GHz. Tyto pásma jsou nasazována pro různé aplikace. Standard sítí 5G definuje tři kmitočtová pásma [5]:

- nízká (low-band, pod 2 GHz),
- střední (mid-band, 2 až 6 GHz),
- vysoká (high-band, 24 až 100 GHz).

Kmitočtové pásmo okolo 700 MHz (low-band) je typické tím, že jeho šířka pásma zásadně limituje objem přenášených dat. Má omezenou maximální dosažitelnou přenosovou rychlost a vysoké zpoždění při přenosu. Toto pásmo je vhodné pro IoT zařízení, která nepotřebují nízké zpoždění při přenosu nebo pro pokrytí rozsáhlých lokalit, kde není požadavek na obsloužení velkého počtu koncových zařízení současně [5].

Kmitočtové pásmo 3,4–3,8 GHz (mid-band) umožňuje přenosové rychlosti ve stovkách Mbit/s. Pokrytí lokalit signálem je menší než u kmitočtového pásma low-band. Toto pásmo umožňuje využít technologii beamforming díky víceprvkovým anténám. Antény pomocí této technologie dokážou signál směrovat na konkrétní zařízení, což šetří spotřebu energie a kapacitu spektra, a tím je zajištěn efektivnější provoz sítě [5].

Kmitočtové pásmo 26 GHz (high-band) podporuje využití milimetrových vln, které umožňují přenosové rychlosti v řádech Gbit/s, nízké zpoždění při přenosu a připojení velkého množství zařízení. Šíření rádiových vln je v řádech stovek metrů. Pro využívání tohoto kmitočtového pásma je potřeba vybudovat mnoho malých základnových stanic (small cells), které jsou napojeny ideálně na optickou síť [5].

2.2.1 Využití kmitočtových pásem v České republice

Český telekomunikační úřad (ČTÚ) dne 7. srpna 2020 spustil výběrové řízení k využívání kmitočtových pásem 700 MHz a 3,4–3,6 GHz [20]. Ty si mezi sebe rozdělily subjekty *CentroNet, a.s*, *Nortic Telecom 5G a.s.*, *O2 Czech Republic a.s.*, *T-Mobile Czech Republic a.s.* a *Vodafone Czech Republic a.s.* (viz tabulka 2.1). Dne 11. srpna 2020 ČTÚ započal veřejnou konzultaci k návrhu [21] části plánu využití kmitočtových pásem 24,25–27,5 GHz. ČTÚ v tomto návrhu zpřístupnil v kmitočtovém pásmu 26 GHz ucelený úsek o šířce 1 GHz pro poskytování ultra-vysokorychlostních služeb. Motivací bylo vytvoření prostoru pro inovativní využití tohoto kmitočtového pásma a také umožnění praktického ověřování technických řešení pro účely poskytování veřejně dostupných služeb a dalších aplikací. Připomínky k tomuto návrhu mohly subjekty podávat do 11. září 2020.

K tomuto návrhu se vyjádřily subjekty *T-Mobile Czech Republic a.s.*, *Qualcomm Communications SARL*, *MBC Czech Republic s.r.o.* a *Vodafone Czech Republic a.s.* Subjekt *T-Mobile Czech Republic a.s.* uvedl v závěru dokumentu pro uplatnění připomínek, stanovisek a názorů [22]: *„Z uvedeného je zřejmé, že v uvolnění pásma 26 GHz není obecně priorita ani pro rok 2020, ani pro nejbližší roky. Naopak považujeme za nutné, aby se před samotným zpřístupněním pásma udála*

celá řada dílčích opatření/kroků tak, aby toto milimetrové pásmo mohlo skutečně sloužit jako pásmo pro významný rozvoj 5G a v mezidobí nedošlo k jeho neefektivnímu využití, které zablokuje jakékoliv další využití. Jsme přesvědčeni, že reálná potřeba zpřístupnění pásma 26 GHz se ukáže až po zavedení primárního 5G pásma, tedy pásma 3.X GHz, a jeho uplatnění pro skutečně 5G komerční modely. Pro výše uvedené důvody žádáme Český telekomunikační úřad, aby konzultaci v současné chvíli zastavil a k diskuzi o podmínkách využití pásma 26 GHz se vrátil až po alokaci pásma 3.X GHz a jeho následném použití při rozvoji sítí. V opačném případě je nutné se vypořádat minimálně s nedořešenými otázkami předloženými v rámci připomínek výše.“

Subjekt *Vodafone Czech Republic a.s.* v závěru dokumentu pro uplatnění připomínek, stanovisek a názorů uvedl [23]: *„Vzhledem k výše uvedenému máme za to, že z pohledu 5G není v tuto chvíli jasná nutnost a potřebnost otevření uvažovaného úseku 26,5–27,5 GHz. V Návrhu není uvedeno, zda ČTÚ již eviduje zájem poskytovatelů služeb o jeho zpřístupnění ke komerčnímu využití, zejména pro 5G. Proto společnost Vodafone žádá o přerušení aktivit směřujících ke změně dotčeného PVRS a znovuotevření diskuse nejdříve koncem roku 2021.“*

Dne 13. října 2020 rada ČTÚ schválila opatření pro zpřístupnění úseku kmitočtového pásma 26 GHz k experimentálnímu provozu budoucích sítí 5G. Zájemci podle něj budou moci na základě individuálního oprávnění v kmitočtovém pásmu 24,25–27,5 GHz pokusně využívat úsek o šířce 1 GHz. Získané zkušenosti mají v budoucnu pomoci stanovit způsob, jakým se kmitočtové pásmo 26 GHz zpřístupní k budoucímu komerčnímu využívání v sítích 5G. V závěru dokumentu ČTÚ je uvedeno [24]: *„Důvodem pro zavedení podmínek pro experimentální provoz IMT/5G je aktuální absence bezprostřední tržní poptávky po využití pásma 26 GHz aplikacemi 5G a dále potřeba doplnění dalších technických a plánovacích podmínek, které ale v současnosti není možné dopředu upřesnit bez předchozích zkušeností a údajů o konkrétních technických řešeních 5G.“*

Tabulka 2.1: Výsledky aukce kmitočtových pásem z roku 2020 [20].

Vítěz aukce	Přidělené úseky kmitočtů v pásmu 700 MHz	Přidělené úseky kmitočtů v pásmu 3,5 GHz
O2 Czech Republic a.s	703–713 / 758–768 MHz	3540–3560 MHz
T-Mobile Czech Republic a.s.	713–723 / 768–778 MHz	3480–3540 MHz
Vodafone Czech Republic a.s.	723–733 / 778–788 MHz	3560–3580 MHz
CentroNet, a.s	-	3400–3480 MHz
Nordic Telecom 5G a.s.	-	3580–3600 MHz

2.3 Využití sítí 5G v průmyslu

Etapa 5G SA má díky svým vlastnostem ideální předpoklady pro tvorbu privátních sítí 5G (kampusových sítí), které mají klíčové uplatnění v průmyslu. Jedná se o soukromou síť pokrývající vnitřní i venkovní oblasti, ke které lze pomocí specifických SIM karet připojovat různá zařízení. Výhodou této sítě je, že je plně dedikována pro jednoho daného zákazníka pro interní použití. Dle požadavků je tedy nastavené vlastní jádro a hardware. Díky tomu má zákazník absolutní kontrolu nad svou komunikační sítí.

Privátní síť 5G je flexibilní a přináší značné výhody ve spolehlivosti a v možnosti propojit cokoliv s čímkoliv, což dává prostor možnostem pro zefektivnění výroby, zabezpečení fungování kritické infrastruktury nebo pro zvýšení produktivity firmy. Další výhodou je, že privátní síť je oddělená například od veřejných mobilních sítí a Wi-Fi sítí. To znamená, že se při přetížení navzájem tyto sítě negativně neovlivňují. Nevýhodou těchto sítí je, že ne všechny koncová zařízení jsou kompatibilní s 5G standardy. Tedy je nutné investovat do nových zařízení a platit za licenční kmitočtové pásmo.

Nasazení privátní sítě je vhodné například ve výrobních halách a firmách, které chtějí nebo již provozují počítačem řízené stroje, roboty či autonomní vozítka. Dále je vhodná i pro logistické společnosti, kterým tato síť pomůže zajistit lepší organizaci jejich dep. Privátní sítě 5G nabízí [14]:

- propojení velkého množství senzorů, čidel, autonomních vozidel a výrobních zařízení v areálu (zvýší se efektivita a bezpečnost),
- nízké zpoždění při přenosu dat (například umožní zaměstnancům práci v prostředí rozšířené nebo virtuální reality a zajistí plynulý obraz),
- přenosovou rychlost dat až 10 Gbit/s,
- nahrávání velkého množství dat,
- možnost venkovního pokrytí,
- úsporu nákladů i času při školení pracovníků pomocí rozšíření reality,
- prediktivní údržbu (řízené umělou inteligencí),
- předcházení omezení standardního provozu výrobních linek,
- sledovaní a optimalizování výroby v reálném čase,
- sběr dat z výrobních strojů v reálném čase,
- trasování a sledování, tedy přesnou geolokaci zařízení, stroje nebo materiálu ve výrobní hale či skladu v reálném čase,
- zabezpečení a spolehlivost.

Výrobní sítě se především skládají z enormního množství aktuátorů či senzorů a dalších zařízení, které spolu spolupracují a generují i zpracovávají velký objem dat, jako například informace o poloze objektů z různých zdrojů. Tato data jsou běžně ukládána pomocí cloudových služeb a mohou být i zpracovávána

za pomoci cloudových výpočtů. Privátní sítě 5G jsou vhodnou součástí podpory služeb (aplikací), které jsou využívány v rámci konceptu *Průmysl 4.0* [14]:

- **Monitorování a řízení v reálném čase** poskytuje nepřetržité monitorování a řízení průmyslových procesů a zařízení pomocí senzorů. Umožňuje včasnou detekci anomálií nebo odchylek, což zajistí rychlou reakci pro zajištění nepřetržité výroby. Tento systém vyžaduje nízké zpoždění při přenosu (1 až 10 ms) a vysokou přenosovou rychlost do 1 Gbit/s.

- **Digitální dvojče** slouží pro simulaci současných či budoucích výrobních zařízení pro optimalizaci a testování. Umožňuje ověřit, že vše bude fungovat tak, aby se neohrozila současná výroba. Vytvoření digitálního dvojčete výrobního zařízení zlepší efektivitu testování a sníží prostoje bez dopadu na reálnou fyzickou výrobní linku. Tato aplikace vyžaduje vysokou přenosovou rychlost 500 Mbit/s až 1 Gbit/s.

- **Prediktivní údržba** využívá senzory a analýzu dat k předpovídání poruch zařízení za pomoci umělé inteligence a strojového učení. Díky tomu může systém proaktivně plánovat činnosti údržby a minimalizovat prostoje výrobní linky. Pro tuto aplikaci je vhodná přenosová rychlost v rozsahu od 100 Mbit/s do 1 Gbit/s.

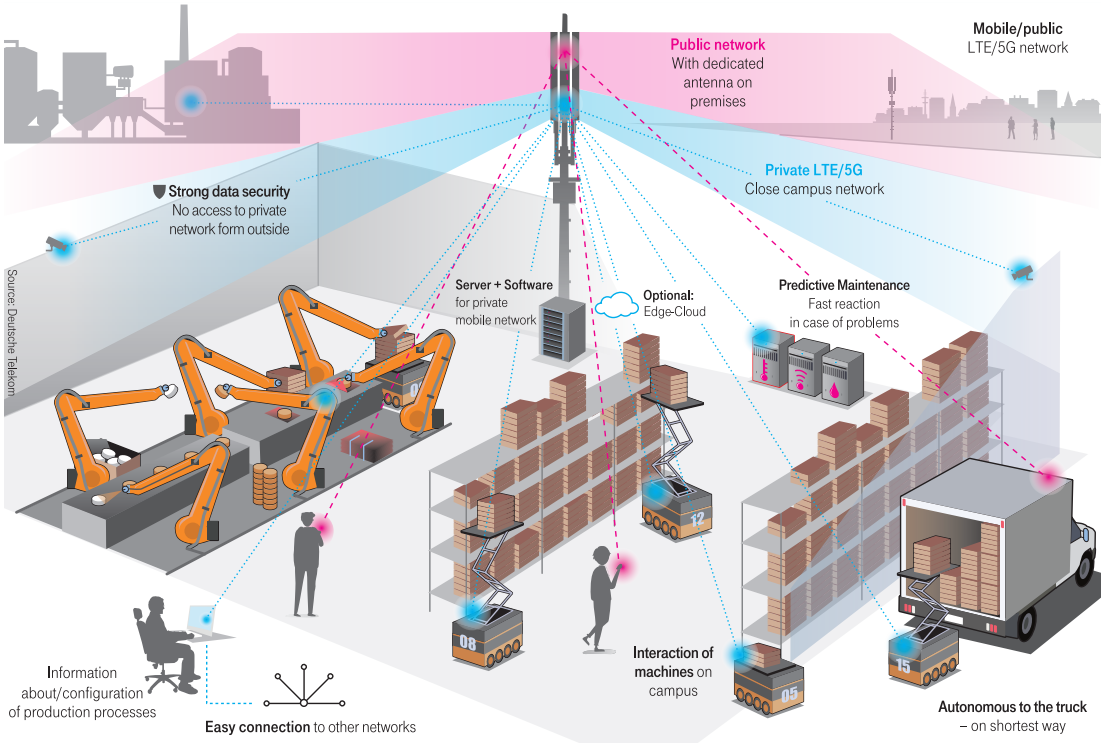
- **Monitorování dodavatelského řetězce** se implementuje integrací zařízení IoT pro sledování a monitorování pohybu zboží. Dochází k poskytování dat v reálném čase o stavu zásob a harmonogramech dodávek, které mohou být poskytnuty všem zúčastněným stranám. Tato služba vyžaduje střední přenosovou rychlost 100 až 500 Mbit/s.

- **Rozšířená realita** umožňuje poskytnutí vzdálené pomoci pro odstraňování problémů, údržby a školení. Odborník může navigovat nebo školit pracovníky v reálném čase, aniž by byl fyzicky přítomen. Tato aplikace vyžaduje nízké zpoždění při přenosu (1 až 10 ms) a vysokou přenosovou rychlost (až 1 Gbit/s).

- **Autonomní vozidla a drony** se využívají pro manipulaci s materiálem, správu zásob, video analýzu a dohled. Umožňují zvýšit efektivitu logistiky a minimalizaci manuálních zásahů. Vyžadují nízké zpoždění při přenosu (1 až 10 ms) a přenosovou rychlost v rozsahu od 100 Mbit/s do 1 Gbit/s.

- **Roboti** v továrně jsou nasazeni pro spolupráci při montáži nebo balení nějakých předmětů. Vyžadují nízké zpoždění při přenosu (1 až 10 ms) a vysokou přenosovou rychlost (500 Mbit/s až 1 Gbit/s) pro plynulou spolupráci a okamžitou reakci na dynamické prostředí.

Rozvoj privátních sítí 5G (kampusových sítí) otevírá mobilním operátorům nové příležitosti pro nabídky služeb a zdroj příjmů. Firmám lze například poskytovat specificky nastavené jádro, přesné lokační služby a komponenty sítě s garantovanou úrovní kvality služeb. To všechno pomáhá firmám zvyšovat efektivitu a snižovat náklady [25]. Například mobilní operátor *T-mobile Czech Republic a.s.* nabízí vybudování kampusové sítě (viz obrázek 2.4), která využívá převážně technologie společnosti *Ericsson spol. s.r.o.*



Obrázek 2.4: Příklad kampusové sítě – privátní sítě 4G/5G [26].

2.4 Porovnání privátních sítí 5G s Wi-Fi sítěmi

Za dobu existence Wi-Fi sítí vzniklo mnoho variant standardů pod označením IEEE 802.11x, kde „x“ označuje variantu standardu (viz tabulka 2.2). Nejnovější verze Wi-Fi 6 řeší problémy starších variant, mezi které se řadí především nízký počet připojených zařízení nebo rušení od okolních přístupových bodů. Wi-Fi sítě byly navrhnuty jako náhrada strukturované kabeláže a pro poskytnutí mobility v rámci budov. Vytváří bezdrátovou komunikační infrastrukturu pro zařízení, která jsou využívána v domácnostech, firmách nebo v průmyslu (například pro počítače, stroje, senzory, aktuátory, roboty, vozíky či kamery) [19].

V současné době, zejména v České republice, jsou Wi-Fi sítě využívány i pro realizaci vzdálených připojení a venkovních směrových spojů. Řadí se mezi typické bezdrátové technologie, které se využívají v přístupových sítích. Tento model připojení je hojně využíván kvůli nízkým nákladům na realizaci a také poskytuje dostačující přenosové parametry pro nenáročné uživatele. V případě definice bezdrátových Wi-Fi sítích je nutné rozlišovat, zda se jedná o veřejnou datovou síť poskytovatele zajišťující připojení koncového účastníka k Internetu nebo o lokální Wi-Fi síť účastníka za koncovým bodem veřejné datové sítě [19].

Dedikované privátní sítě 5G mají především díky svým vlastnostem ambici nahradit Wi-Fi sítě v průmyslu nebo může být běžné, že tyto dvě sítě budou provozovány společně v závislosti na potřebách firmy. Liší se v mnoha aspektech, mezi hlavní se řadí [27, 28]:

- kmitočtové pásmo (licenční a bezlicenční),
- spolehlivost,
- predikovatelnost,

- zpoždění při přenosu,
- počet připojených koncových zařízeních,
- mobilita,
- zabezpečení.

Wi-Fi sítě využívají kmitočtové pásmo 2,4 GHz a 5 GHz, což jsou bezlicenční pásma. Tedy tato pásma lze ihned začít využívat bez povolení a poplatků, avšak je nutné počítat s rušením z jiných zdrojů a s nižším odstupem signálu od šumu. Existuje i rozšíření Wi-Fi 6E, které navíc umožňuje kmitočtové pásmo 6 GHz. Pro privátní sítě 5G jsou využívána kmitočtová pásma 3,4–3,8 GHz a případně i 26 GHz, což jsou licenční pásma, u kterých není kvůli legislativě jednoduché a přímočaré jejich nasazení. Výhodou licenčních pásem je to, že dostupnost šířky pásma lze garantovat, a tím zajistit vyšší přenosovou rychlost a spolehlivost sítě [27].

Tabulka 2.2: Varianty standardu Wi-Fi [19].

Označení varianty	Rok vydání	Frekvenční pásmo [GHz]	Šířka kanálu [MHz]	Teoretická přenosová rychlost [Mbit/s]
802.11a (Wi-Fi 2)	1999	3,7; 5	20	54
802.11b (Wi-Fi 1)	1999	2,4	20	11
802.11g (Wi-Fi 3)	2003	2,4	20	54
802.11n (Wi-Fi 4)	2009	2,4; 5	20; 40	600
802.11ac (Wi-Fi 5)	2014	5	20; 40; 80; 160	867
802.11ax (Wi-Fi 6)	2019	2,4; 5	20; 40; 80; 160	11 000

Při rozhodování, zda využít privátní síť 5G nebo Wi-Fi síť, je nutné stanovit, zda síť bude sloužit pro kritické či nekritické aplikace. Wi-Fi sítě jsou vhodné pro vybudování sítě pro nekritické aplikace. Například jsou požadavky na mobilitu, nikoliv na stabilní nízké zpoždění při přenosu, které je potřebné pro rychlé reakce v reálném čase na nějakou událost. Privátní sítě 5G jsou naopak vhodné pro kritické aplikace, které vyžadují nízké zpoždění při přenosu (v řádu jednotek milisekund), vysokou spolehlivost a dodržení SLA (Service Level Agreement). Například na této síti může záviset výrobní linka, kde výpadek produkce může znamenat vysoké ztráty [28].

Pro kritické aplikace lze využít Wi-Fi sítě, avšak její vlastnosti nejsou pro toto nasazení vyhovující. Zpoždění při přenosu u Wi-Fi sítí se neliší řádově, ale může výrazně kolísat v čase. Nelze tedy garantovat ani predikovat. Dále hlavními důvody jsou případné kolize způsobující ztrátovost paketů kvůli bezlicenčnímu pásmu nebo kvůli počtu zařízení, která jsou k síti připojená. Wi-Fi sítě umožňují připojit řádově desítky koncových zařízeních a privátní sítě 5G umožňují značně vyšší počet připojených koncových zařízení [28].

Požadavek na mobilitu je klíčový pro robotická vozítka nebo autonomní roboty, kteří se pohybují po továrně. V privátních sítích 5G je zajištění mobility robustnější než u Wi-Fi sítí. V privátních sítích 5G si koncová zařízení monitorují základnové stanice v okolí a pokud kvalita signálu přesáhne určitou hranici, tak se provede handover (změna základnové stanice kvůli pohybu koncových zařízení pro nepřetržité spojení), a tím udržovat určitou úroveň kvality služeb. U Wi-Fi sítí je běžné, že koncové zařízení je připojeno k přístupovému bodu, dokud neztratí signál, bez ohledu na to, že se již nachází v zóně se silnějším signálem od jiného přístupového bodu. Tedy až po ztrátě signálu dochází k využívání jiného přístupového bodu. Jsou nasazovány mechanismy, které mají tento nedostatek řešit a odpojit koncové zařízení dříve, ale není to tak kvalitní provedení jako u privátních sítí 5G [28].

Obě tyto sítě poskytují zabezpečený komunikační kanál, avšak privátní sítě 5G nabízí robustnější zabezpečení, protože jejich hlavním prvkem bezpečnosti je SIM karta, bez které se koncová zařízení do sítě nepřipojí. Obsahuje klíče pro identifikaci a autentizaci zařízení v síti. Možnost útoku na síť lze realizovat tím, že by útočník SIM kartu fyzicky z koncového zařízení vyjmul a zneužil pomocí svého zařízení. Wi-Fi sítě jsou zabezpečeny na úrovni klíče, který je společný pro celou síť či pro každé koncové zařízení zvlášť. Další možnost je ověření pomocí RADIUS (Remote Authentication Dial In User Service) serveru. Hlavní příčinou zranitelností Wi-Fi sítí jsou nedokonalosti v protokolech WPA (Wi-Fi Protected Access) i WPA2. Existují i útoky na Wi-Fi sítě, které mohou být založeny na „podvodném přístupovém bodu“ nebo „phishing přístupovém bodu“ [28].

2.5 Pokrytí signálem v průmyslových areálech

Umístění přístupových bodů pro pokrytí v průmyslových areálech má dvě hlavní roviny:

- pokrytí určitého prostoru signálem,
- kapacitní plánování pro služby (aplikace) využívané v průmyslu.

Například z hlediska pokrytí signálem nějakého areálu stačí čtyři přístupové body, ale nebude dostatečná přenosová kapacita pro využívání vysokého počtu zařízení anebo nebude umožněna geolokace zařízeních. Tedy plánování pokrytí je závislé na konkrétních požadavcích na služby pro daný areál. Při stanovení počtu, umístění a koncentrace přístupových bodů v areálech je nutné brát v úvahu [29]:

- počet připojených senzorů a dalších zařízení v různých částech areálu (například některá zařízení mohou být i v pohybu jako jsou autonomní roboti či digitální vozítka),

- zajištění úrovně QoS a dodržení SLA, především pro kritické aplikace (například brát v potaz části areálu, kde budou provozovány služby vyžadující spolehlivost a nízké zpoždění při přenosu),
- slabá místa (například boční místnosti či rohy areálů),
- uspořádání, strukturu areálu a případné zdroje rušení,
- možné selhání přístupového bodu (zavést redundanci).

Během budování privátní sítě 5G je užitečné sledovat parametry signálu, a tím odhalit problémová místa a případně dle potřeby přidat více přístupových bodů. Mezi hlavní soubor parametrů signálu sloužící pro posouzení kvality patří [30, 31]:

- **RSSI** (Received Signal Strength Indication) je indikátor intenzity přijímaného signálu:
  - velmi dobré: RSSI > -65 dBm,
  - dobré: -65 dBm $\leq$ RSSI < -75 dBm,
  - slabé: -75 dBm $\leq$ RSSI < -85 dBm,
  - velmi slabé: RSSI $\leq$ -85 dBm.
- **RSRQ** (Reference Signal Receive Quality) představuje ukazatel kvality přijímaného referenčního signálu:
  - velmi dobré: RSRQ $\geq$ -10 dB,
  - dobré: -10 dB < RSRQ $\leq$ -15 dB,
  - slabé: -15 dB < RSRQ < -20 dB,
  - velmi slabé: RSRQ $\leq$ -20 dB.
- **RSRP** (Reference Signal Receive Power) je úroveň výkonu přijímaného referenčního signálu:
  - velmi dobré: RSRP $\geq$ -80 dBm,
  - dobré: -80 dBm < RSRP $\leq$ -90 dBm,
  - slabé: -90 dBm < RSRP < -100 dBm,
  - velmi slabé: RSRP $\leq$ -100 dBm.
- **SINR** (Signal to Interference plus Noise Ratio) představuje odstup signálu od interferencí a šumu:
  - velmi dobré: SINR $\geq$ 20 dB,
  - dobré: 13 dB $\leq$ SINR < 20 dB,
  - slabé: 0 dB < SINR < -13 dB,
  - velmi slabé: SINR $\leq$ 0 dB.

Pro privátní sítě 5G v Evropě jsou využívána kmitočtová pásma 3,4–3,8 GHz a nejspíše v budoucnu bude nasazeno kmitočtové pásmo 26 GHz. Využívané pásmo má zásadní vliv na parametry sítě (viz podkapitola 2.2). Kapacita komunikačního kanálu (Shannon-Hartleyův teorém) v bit/s je dána vztahem

$$C = B \cdot \log_2 \left(1 + \frac{S}{N}\right), \tag{2.1}$$

kde B je šířka kmitočtového pásma kanálu v Hz a S/N je poměr výkonu užitečného signálu k šumu v přenosovém kanálu. Také je nutné zajisti při tvorbě privátní sítě 5G to, aby tzv. *úzké hrdlo* bylo vytvořeno bezdrátovou síť, a ne například nízkou výkonností serverů nebo nevhodným výběrem kabelů, které připojují přístupové body.

3. Problematika QoS a diferenciace služeb

Kvalita neboli jakost služeb (QoS – Quality of Services) je komplexní pohled na služby, který je specifikován ITU-T. Tyto specifikace následně přebírají poskytovatelé služeb. ITU-T v doporučení E.800 [32] definuje QoS jako: „*Souhrn vlastností telekomunikační služby, které mají vliv na její schopnost splňovat stanovené nebo implicitní potřeby uživatele služby.*“ Také ETSI (European Telecommunications Standards Institute) v technické zprávě [33] definuje QoS z pohledu datové sítě jako: „*Schopnost segmentovat síťový provoz nebo rozlišovat typy provozů tak, aby síť zacházela s určitým provozem jinak než s ostatními.*“

Cílem QoS je pomocí sady nástrojů a technik poskytovat služby (doručení dat) na určité úrovni a dodržovat SLA (Service Level Agreement), aby poskytovatel služeb neplatil pokuty pro nedodržování sjednané smlouvy. QoS je ovlivněno všemi komponentami sítě jako jsou například směrovače, přepínače, servery a přenosová média. ITU-T v doporučení I.350 [34] popisuje obecnou výkonnostní matici 3×3, která bere v potaz kritéria (rychlost, přesnost a spolehlivost) a fáze (sestavení spojení, přenos informace a zrušení spojení). Existují i komplexnější výkonnostní matice 7×11 dle ITU-T v doporučení E.802 (viz obrázek 3.1).

		Kvalitativní kritéria QoS						
Fáze		Rychlost	Přesnost	Dostupnost	Spolehlivost	Bezpečnost	Jednoduchost	Pružnost
Řízení služby	Prodej a před-smluvní aktivity							
	Poskytování							
	Změna							
	Servisní podpora							
	Oprava							
	Ukončení							
Kvalita spojení	Sestavení spojení							
	Přenos informace							
	Zrušení spojení							
Účtování								
Řízení sítě zákazníkem								

Obrázek 3.1: Komplexní výkonnostní matice 7×11 [35].

QoS bylo tradičně z pohledu koncového uživatele při telefonování. S příchodem nových typů technologií pro komunikaci je nutné brát v potaz to, že ne všechny služby jsou stejné (například IoT). Služby nemusí vyžadovat doručení v reálném čase a příjemce nebo odesílatel dat může být člověk či stroj. I s podobnými

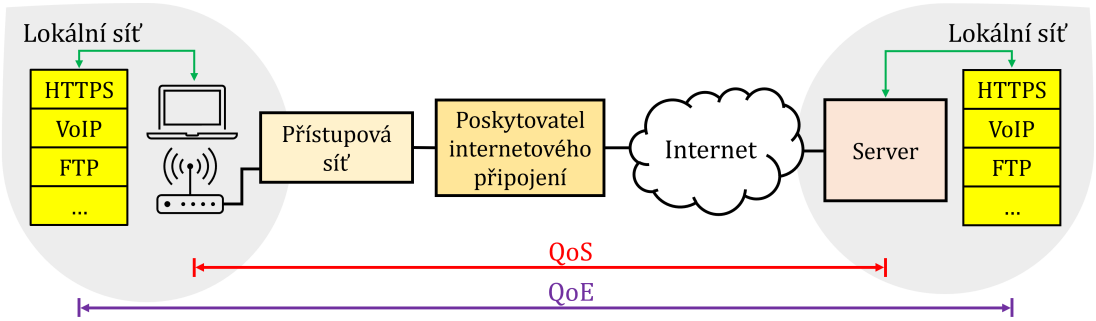
službami lze zacházet různými způsoby v závislosti na tom, zda je využívají lidé nebo stroje [36].

QoS je posuzováno pomocí parametrů (ukazatelů). Mezi základní parametry kvality při přenosu digitálního signálu patří [36]:

- bitová chybovost,
- bloková chybovost,
- zpoždění při přenosu,
- kolísání zpoždění při přenosu,
- četnost ztracených paketů.

Například pro interaktivní službu VoIP (Voice over Internet Protocol) je jedním z důležitých parametrů zpoždění při přenosu. Správce sítě může pro provoz služby VoIP nastavit vyšší prioritu a upřednostnit tak její síťový provoz, aby nebyla zhoršena kvalita při zahlcení média, tedy omezit vybrané služby ve prospěch jiných. QoS je typicky realizováno na směrovačích, kde jsou zahazovány pakety, které přesahují nastavené parametry datových toků.

QoS nesouvisí přímo se zákazníkem, ale týká se média a sítě samotné. Měřítko QoE (Quality of Experience) bere v potaz zkušenosti koncového uživatele se službou, zařízením uživatele a síťovou infrastrukturu (viz obrázek 3.2). Tedy nabízí subjektivní zhodnocení uživatelských očekávání a pocitů na konkrétní služby. Meřítko je využíváno například pro posouzení webové stránky, videa, telefonování a gamingu [37].



Obrázek 3.2: Hranice pro posuzování QoS a QoE v síti [36].

Mezi specifikace QoS parametrů se řadí [36]:

- jednoznačný název (například střední hodnota doby čekání),
- jednoznačná definice (například k čemu se to vztahuje),
- zdroj získávání údajů (například z logů call centra nebo od zákazníka),
- způsob získávání údajů (kde a jak se bude měřit),
- četnost vyhodnocení (doba sledování),
- způsob nezávislé kontroly (kdo bude posuzovat plnění závazů ve smlouvě),

- cílová hodnota (například pravděpodobnost doby čekání déle než určitý čas),
- trend vývoje (zda se blíží hodnota k cíli nebo dochází ke zhoršení či zlepšení),
- prezentace výsledků (například ve formátu CSV nebo JSON).

3.1 Příčiny narušení QoS

Mezi typický síťový provoz patří například interaktivní služby, data managementu sítě, data směrovacích protokolů, kritické aplikace a video na požádání. Tyto služby mají rozdílné požadavky na přenosovou rychlost, zpoždění při přenosu a na ztrátu paketů. Tedy mezi příčiny, které hlavně degradují kvalitu služeb jsou:

- nedostatečná přenosová rychlost (příčinou rostoucího zpoždění při přenosu a ztráty paketů),
- ztráta paketů (intenzita příchozích paketů překročí dostupnou kapacitu odchozího rozhraní),
- stav síťových prvků a jednotlivých rozhraní v přenosové cestě,
- zpoždění při přenosu a jeho rozptyl.

Rozptyl zpoždění (doba přenosu sítí) neboli jitter v IP sítích popisuje nepravidelnost příchodů paketů. Pakety multimediálních toků obvykle přichází do sítě v pravidelných intervalech. Nicméně do svého cíle mohou dorazit s různým zpožděním, v jiném pořadí, vícekrát anebo vůbec. Rozdílné cesty přenosu v síti jsou příčinou nejednotného zacházení s jednotlivými pakety [38, 39].

3.1.1 Klasifikace zpoždění v IP sítích

Zpoždění při přenosu v IP sítích je klasifikováno do těchto skupin [40]:

- **Doba zpracování** (Processing Delay) je doba potřebná pro analýzu záhlaví paketů a přesun paketů ze zásobníku vstupního rozhraní do zásobníku výstupního rozhraní. Řadí se do kategorie proměnného zpoždění, které je dáno síťovým prvkem jako je například přepínač nebo směrovač.
- **Prioritizační zpoždění** (Queuing Delay) znamená zpoždění způsobené prioritizací paketů. Je způsobené změnou pořadí zpracování paketů dle prioritizačních pravidel. Také patří do kategorie proměnného zpoždění.
- **Serializační zpoždění** (Serialization Delay) značí dobu potřebnou pro odeslání paketu na fyzické rozhraní. Řadí se do kategorie fixního zpoždění, které je dáno přenosovým médiem.
- **Doba šíření signálu přenosovým médiem** (Propagation Delay) představuje čas přenosu paketu přenosovým médiem, které je dáno fyzikálními limity a také patří do kategorie fixního zpoždění.

3.1.2 Minimalizace zpoždění v IP sítích

Zpoždění při přenosu je v IP sítích klíčové například pro interaktivní nebo kritické aplikace. Dále ovlivňuje celkovou uživatelskou zkušenost s aplikací. Mezi možnosti, jak minimalizovat zpoždění a jeho rozptyl v IP sítích patří [41, 42, 43]:

- **Zvýšení přenosové rychlosti na rozhraní** – Dochází ke snížení zpoždění umístění paketu na přenosové médium, avšak tato možnost je například u rádiových spojů fyzikálně nemožná kvůli vlastnostem kmitočtových pásmem.

- **Nastavení prioritizace** – Dochází k upřednostňování vybraných služeb (například interaktivních služeb) na úkor zbylých služeb, které například nejsou tak citlivé na zpoždění.

- **Komprese záhlaví paketu** – Směrovače se nastaví tak, že místo části záhlaví paketu druhé nebo třetí vrstvy referenčního modelu ISO/OSI dají nějaký identifikátor například o velikosti 4 bytů. Využívá se to u pomalých spojů, tedy především klesne serializační zpoždění u rozhraní s nízkou přenosovou rychlostí. Nevýhodou je, že vznikne zpoždění, které je způsobené touto kompresí a následnou dekompresí.

- **Fragmentace s prokládáním** – Zpoždění je minimalizováno díky tomu, že je zavedena fragmentace a systém s prioritami. Principem fragmentace je rozdělení jednoho velkého paketu na více paketů. Těmto nově vzniklým paketům je nutné přidat záhlaví, což zatíží rozhraní, a tím se sníží efektivita přenosu. S aktivovanou fragmentací neprojde na rozhraní paket větší, než je nastaveno. Například FTP paket o teoretické velikosti 1500 bytů je fragmentován na tři pakety o velikosti 500 bytů a VoIP paket o velikost 100 bytů s vyšší prioritou nebude čekat déle, než je obsluha FTP paketu o velikost 500 bytů. Právě díky fragmentaci a zavedení priorit je VoIP paket vložen mezi rozdělené FTP pakety (to je princip fragmentace s prokládáním). V prostředí IP není absolutní priorita, tedy to, co je na rozhraní, se musí již odeslat. Fragmentace s prokládáním je vhodná pro pomalé spoje stejně jako komprese záhlaví paketu.

3.2 Modely QoS

Modely QoS představují sadu schopností pro zajištění určité úrovně služby. Modely se liší v tom, jak umožňují službám posílat data a jakými způsoby se síť pokusí tato data doručit do cíle. Například jeden model lze použít pro interaktivní služby, jako je VoIP a video konference, zatímco jiný model je vhodnější pro přenos e-mailů a souborů. Například software Cisco podporuje tři typy modelů [43]:

- **Best Effort Service** je model, při kterém není garantován přenos paketů do cíle a nejsou rozlišovány typy služeb. V tomto modelu jsou všechny služby na stejné úrovni, a tak si toky mezi sebou konkurují o jednu společnou přenosovou rychlost při nějakém zpoždění, ztrátě paketů a zabezpečení. Není tak zaručena žádná úroveň QoS. Je zde uplatňován režim fronty FIFO (First In First Out).

- **Integrated Services** označuje model, který je tokově orientován na konkrétní jedno spojení, a to garantuje QoS. Umožňuje detailní nastavení požadované úrovně QoS pro každou službu (End to End). Je zde možnost rezervace přenosových prostředků a omezení intenzity služeb. Tento model je neaplikovatelný pro rozsáhlé sítě (neškálovatelný), protože každý směrovač musí udržovat informaci o stavu všech toků. Čím více toků, tím jsou vyšší nároky na výkonnost hardwaru. Model má možnosti ověřit, zda lze uskutečnit nové spojení. Tedy musí být garantováno, jestli například daný hovor může vzniknout. Pokud by to síť nezvládla, tak nové spojení nevznikne a probíhající spojení nebudou ovlivněna.
- **Differentiated Services** představuje model, který je agregačně orientován. Pakety služeb jsou rozřazeny do teoreticky 64 tříd a v každém uzlu sítě jsou dána pravidla, jak na pakety z určité třídy reagovat. Například je vytvořena třída zajišťující nízké zpoždění, což je vhodné pro interaktivní služby. Pro značkování, na 3. vrstvě referenčního modelu ISO/OSI, bylo upraveno záhlaví protokolu IP a přidáno pole DSCP (Differentiated Services Code Point), které je o velikosti 6 bytů. Díky agregaci toků je výkonnostně možné tento model nasadit v rozlehlých sítích typu Internet. Tedy tento model je velmi dobře škálovatelný na rozdíl od modelu Integrated Services. Nevýhoda agregace je, že se v rámci třídy toky nerozlišují mezi sebou a kvůli tomu model negarantuje úroveň QoS. Pokud toky ve třídě narostou na určitou mez, tak si toky v rámci jedné třídy začnou konkurovat a vzájemně poškozovat, což má za následek rostoucí ztrátovost paketů (degradaci služeb).

3.3 Metody zajištění QoS

Zajistit QoS lze rezervací přenosové kapacity pro jednotlivé typy služeb nebo dohledem nad zpožděním, rozptylem zpoždění a ztrátovostí paketů. Dále mezi metody, které zajišťují QoS se řadí [43]:

- **Předcházení přetížení**:
  - Random Early Detection,
  - Weighted Random Early Detection.
- **Řízení zahlcení sítě**:
  - Priority Queuing,
  - Custom Queuing,
  - Weighted Fair Queuing,
  - Class Based Weighted Fair Queuing.
- **Omezování a tvarování síťového provozu** (Traffic Policing, Shaping).
- **Vhodnější využití přenosových prostředků**:
  - komprese záhlaví,
  - fragmentace s prokládáním.

3.3.1 Předcházení přetížení

Algoritmy pro předcházení přetížení (Congestion Avoidance) monitorují zatížení rozhraní ve snaze předvídat a vyhýbat se přetížení (přetečení paměti). Pro TCP (Transmission Control Protocol) toky jsou využity algoritmy RED (Random Early Detection) a WRED (Weighted Random Early Detection). Bez těchto algoritmů dochází v případě přetížení rozhraní, kdy paket byl odeslán do plné softwarové paměti (fronty), ke ztrátě paketů, a tím k degradaci služeb. Pro rozhodnutí o zahození paketů z fronty je využit algoritmus *Tail Drop*, který při plné frontě zahazuje jakékoliv další příchozí pakety, dokud není přetížení odstraněno. Ztráta paketů kvůli přetečení paměti může mít například za následky to, že dojde k [43]:

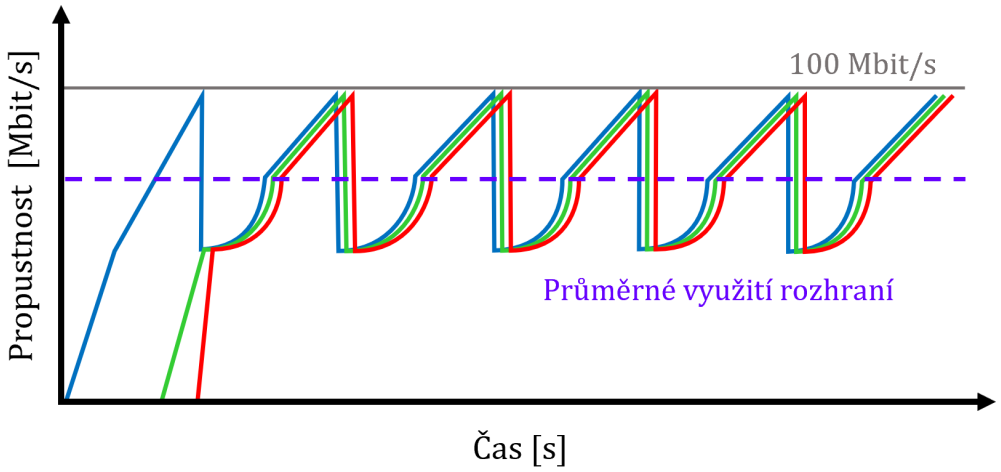
- synchronizaci TCP toků,
- „vyhladovění“ TCP toku agresivnějšími TCP toky,
- nemožnosti rozlišit, který paket bude zahozen.

K synchronizaci TCP toků nastane, pokud po přetečení paměti dojde k omezení TCP toků současně (současné ustoupení ze své rychlosti odesílání paketů) a poté jsou TCP toky restartovány téměř současně, a tak jsou synchronizovány. Tedy TCP toky skoro souběžně zvyšují svou přenosovou rychlost odesílání, což způsobí, že využití rozhraní naroste a znovu nastane jeho zahlcení. Tento cyklus se znovu opakuje (viz obrázek 3.3). To se děje při využívání algoritmu *Tail Drop*. Důsledkem je využití přenosové kapacity ve tvaru pilového zubu na rozhraní, což je příčinou neefektivního využití rozhraní [43].

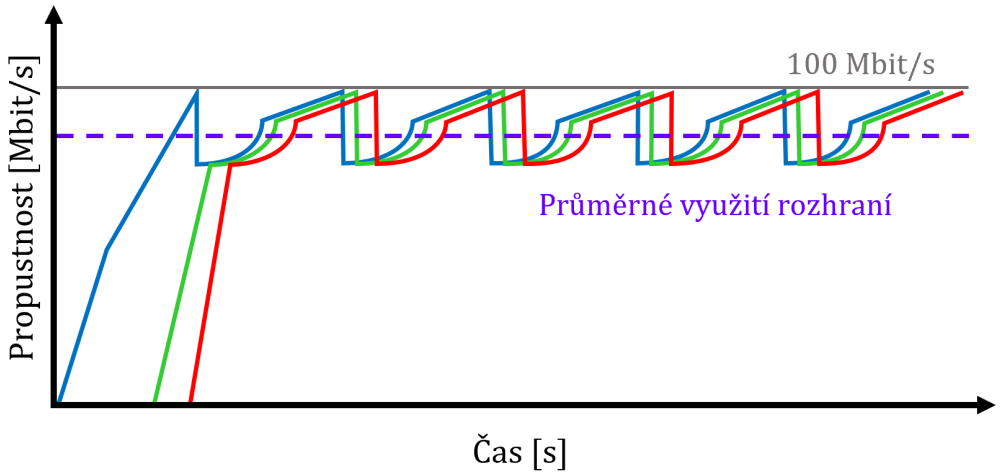
Principem algoritmu RED je to, že jsou při zaplnění paměti (fronty) nad určitou hranici náhodně zahazovány pakety všech toků se stejnou pravděpodobností. Pravděpodobnost ztráty paketů roste se zvyšujícím se využitím paměti. Díky RED jsou TCP toky rozsynchronizovány, a tím bude vyšší průměrné využití kapacity rozhraní (viz obrázek 3.4). Tedy pomalý náběh některých TCP toků nastane dříve díky algoritmu RED než u algoritmu *Tail Drop*. RED funguje v režimech [43]:

- **Beze ztrát** – Využívá se, pokud průměrné využití paměti je mezi nulou a hodnotou „minimum threshold“.
- **Vyhýbání se přetížení** – Je postupem času zvyšována pravděpodobnost ztráty paketů, pokud průměrné využití paměti je mezi hodnotami „minimum threshold“ a „maximum threshold“.
- **Ztráta 100 %** – Využívá se v případě, pokud průměrné využití paměti přesahuje hodnotu „maximum threshold“.

Algoritmus WRED využívá profilů RED, ale při rozhodování o zahození bere v úvahu významnost paketů (IP precedence – priorita paketu, DSCP – Differentiated Services Code Point), čímž podporuje QoS. To znamená, že pravděpodobnost zahození při WRED je ovlivněno nejen mírou naplnění fronty, ale i prioritou paketu. Tedy přednostně jsou zahozeny pakety s nižší prioritou [43].



Obrázek 3.3: Příklad průběhu tří TCP toků před využitím algoritmu RED [43].



Obrázek 3.4: Příklad průběhu tří TCP toků po využití algoritmu RED [43].

3.3.2 Řešení zahlcení

Řešení zahlcení (Congestion Management) slouží k řízení přetížení na odchozích rozhraních, jakmile k němu dojde. Provozům služeb ve frontě je přiřazena třída a jsou využívány různé režimy obsluhy této fronty, tedy výběru dalšího paketu pro odesílání. Například software Cisco podporuje tyto režimy fronty [43]:

- **Priority Queuing** (PQ) je režim fronty založen na principu absolutní priority. To znamená, že pakety zařazené do třídy s vyšší prioritou mají vždy přednost před pakety, které jsou z třídy s nižší prioritou. Jsou zde typicky čtyři třídy s prioritami (vysoká, střední, normální a nízká). Vstupní pakety jsou rozřazeny do těchto tříd tím, že obdrží značku třídy. Na základně této značky jsou pakety pomocí metody ukazatelů z fronty vybírány a odesílány na odchozí rozhraní. Principem je, že pokud se má odeslat paket na rozhraní, tak vždy je vybrán paket z třídy s vyšší prioritou. Nevýhoda tohoto mechanismu je tzv. *monopolizace rozhraní*, což znamená, že třídy s vyšší prioritou mohou získat celou přenosovou kapacitu a třídy s nižší prioritou nemusí mít žádnou. Následkem je, že některé pakety budou stále ve frontě.

- **Custom Queuing** (CQ) je režim fronty založen na principu, kolik která služba z celkové kapacity rozhraní proporcionálně dostane přenosové kapacity. Rozděluje se dostupná kapacita rozhraní mezi třídy (řeší situaci *monopolizace rozhraní* u režimu fronty PQ). Například tři desetiny kapacity se využije pro první třídu, dvě desetiny pro další třídu atd. Využívá se metoda Weighted Round Robin, při které se postupně obcházejí jednotlivé třídy a pokud je pro danou třídu paket ve frontě, tak se odešle na odchozí rozhraní tolik, kolik je definováno pro danou třídu a přijde na řadu další třída. Nevýhoda je, že zde není priorita, která by nějaký paket upřednostnila před ostatními. Tedy nelze nastavit to, které pakety půjdou jako první a není možné garantovat určité minimální zpoždění. Tento režim fronty je nevhodný pro systémy, které vyžadují nízké zpoždění.

- **Weighted Fair Queuing** (WFQ) je režim fronty, který se snaží všem paketům dát stejnou kapacitu, tedy každému spojení garantuje přístup k odchozímu rozhraní, ale negarantuje přenosové rychlosti. Má přednastaveno 256 front a je možné nastavit až 4069 front. Umožňuje automatickou klasifikaci (uživatel konfiguruje jen počet front), při které je každé spojení identifikováno podle parametrů na základě zdrojové adresy, cílové adresy, protokolu, zdrojového portu, cílového portu a IP precedence. Některá spojení mohou spadat do jedné společné fronty (stejný identifikátor toku), pokud počet spojení přesáhne nakonfigurovanou hodnotu front. V tomto případě je ve frontě uplatňován režim FIFO. Při přetížení tento režim fronty zahazuje pakety nejagresivnějších toků.

- **Class-Based Weighted Fair Queuing** (CBWFQ) je rozšířením režimu fronty WFQ o uživatelem definované třídy. Pakety se do tříd nezařazují automaticky, ale dle definice uživatelem. Ve třídách již je možnost rezervace přenosové rychlosti. Je zde využíváno až 64 tříd. Do poslední třídy jsou zařazovány pakety, které klasifikátor neumí roztřídit a na ně je aplikován režim fronty WFQ nebo FIFO. V případě, že pakety určité třídy přichází s vyšší než garantovanou intenzitou, jsou přebytečné pakety zahozeny i pokud není zcela využito odchozí rozhraní.

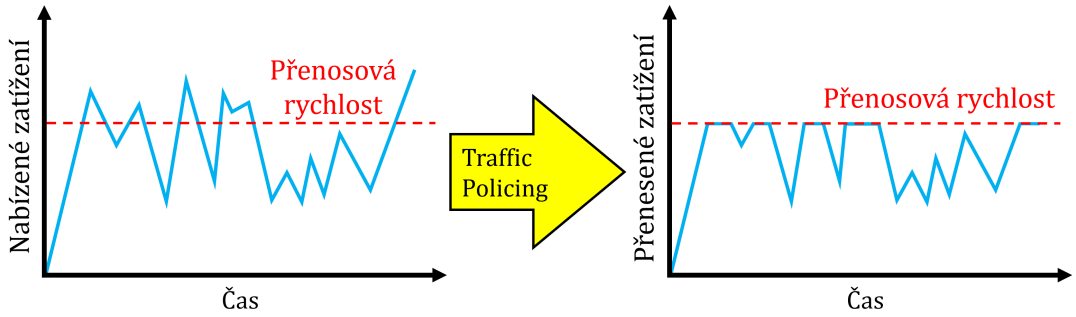
- **Low-Latency Queuing** (LLQ) je rozšířením režimu fronty CBWFQ. Je zde navíc třída, která má nejvyšší prioritu, tedy pakety této třídy jsou vybrány na odchozí rozhraní vždy jako první. Pro tuto třídu se musí nějaká přenosová kapacita z celkové kapacity rezervovat. Například do třídy s nejvyšší prioritou spadají nějaké kritické nebo interaktivní služby a do zbylých tříd se řadí služby například pro databáze. Prioritním třídám je v tomto režimu fronty garantováno minimální zpoždění paketů a maximální dovolená přenosová rychlost. Při překročení garantované meze pro přenosovou rychlost dochází ke ztrátě nadbytečných paketů i u třídy s nejvyšší prioritou.

3.3.3 Omezování a tvarování síťového provozu

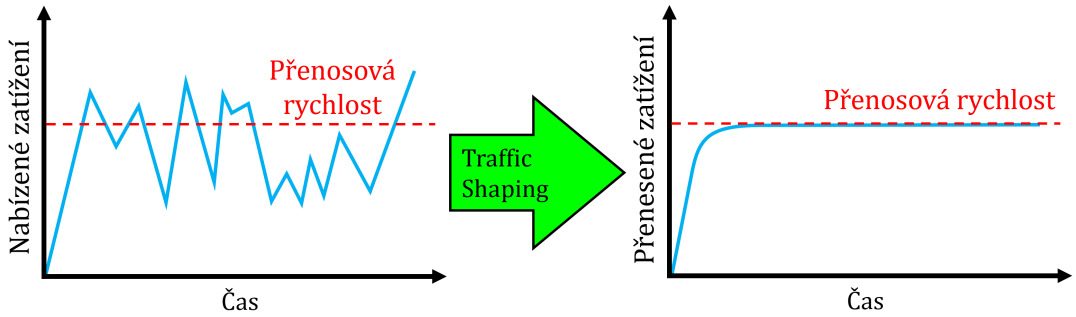
Při nasazení metody omezování síťového provozu (Traffic Policing) dochází k zahození přebytečných paketů pokud nabízené zatížení přesáhne nastavenou mez. Obrázek 3.5 zobrazuje princip této metody, tedy je ořezán provoz, který překračuje mez omezení naznačenou červenou přerušovanou čárou [44].

Metoda tvarování síťového provozu (Traffic Shaping) reguluje síťový provoz, pokud nabízené zatížení dosáhne nastavené meze. Dochází k zadržování paketů ve frontě, které budou později poslány v průběhu času. Tedy může docházet ke zpožďování provozu služeb nebo omezování celkové propustnosti. Obrázek 3.6 zobrazuje princip této metody, tedy výsledkem je rozložený síťový provoz v čase [44].

Metoda tvarování vyžaduje fronty s dostatečnou kapacitou pro ukládání paketů, zatímco metoda omezování ne, protože u této metody dochází k zahazování paketů. Účelem těchto metod je udržovat určitý maximální síťový provoz a nijak není garantována minimální mez pro tento provoz. Například metodu omezování využívají poskytovatelé internetového připojení na určitý příchozí síťový provoz, a naopak metodu tvarování využijí zákazníci na určitý odchozí síťový provoz, aby jejich provoz nebyl zbytečně zahozen kvůli určité mezi stanovené ve smlouvě [43, 44].



Obrázek 3.5: Metoda omezování síťového provozu – Traffic Policing [44].



Obrázek 3.6: Metoda tvarování síťového provozu – Traffic Shaping [44].

3.4 Nasazení VLAN v průmyslu pro diferenciaci služeb

Diferenciace služeb má za cíl upřednostňovat určitý síťový provoz dle požadavků firmy. Služby (aplikace) využívané v průmyslu mají různé nároky například na spolehlivost a zpoždění při přenosu. Jednou ze základních možností pro zajištění diferenciace služeb v privátních sítích 5G je pomocí VLAN (Virtual Local Area Network), což je na úrovni Ethernetu. VLAN slouží k logickému rozdělení sítě bez ohledu na fyzické uspořádání. Tak je skupina koncových zařízení segmentována podle požadavků. Tedy určité využívané služby (aplikace) lze rozdělit do různých VLAN dle potřeby pro zajištění určité úrovně QoS [45].

VLAN je založena na principu značkování dat. Standard IEEE 802.1Q (VLAN tagging) dovoluje rozdělení fyzické sítě na více virtuálních sítí. Dochází k rozšíření hlavičky ethernetového rámce o tzv. *tag*, který specifikuje do jaké virtuální sítě daný rámec patří [45]. Nasazení VLAN v rámci průmyslu především umožňuje:

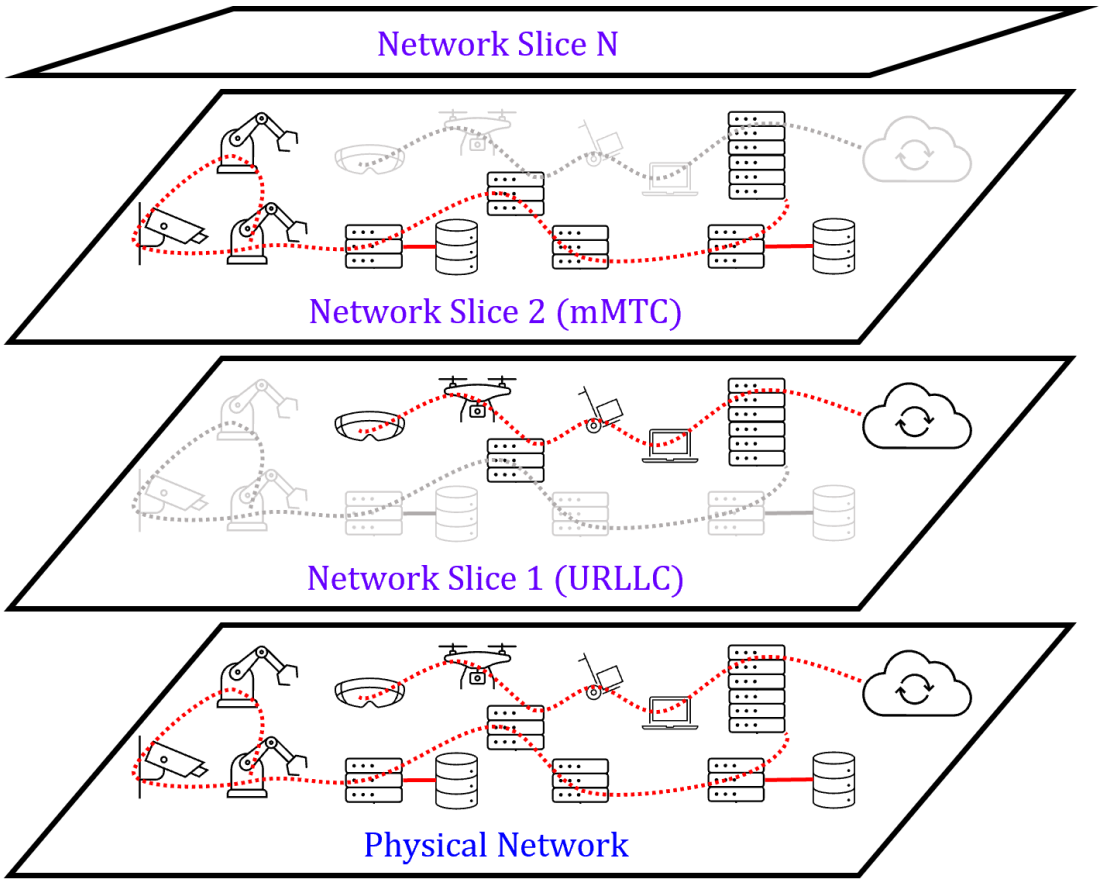
- **Zajištění určité úrovně QoS** – VLAN lze využívat ve spojení s modely QoS k prioritizaci určitého provozu. Například pro kritické aplikace, které vyžadují nízké zpoždění při přenosu.
- **Flexibilitu a škálovatelnost** – Možnost snadno překonfigurovat síť dle měnících se požadavků, jako je přidávání nových senzorů, aktuátorů nebo výrobních linek.
- **Zabezpečení a centralizovanou správu** – Možnost oddělení různých částí síťové infrastruktury.

3.5 Network slicing pro průmysl

Koncept network slicing je podporován jádrem sítě 5G. Umožňuje tvorbu virtuálních vrstev, které jsou různě nastaveny dle potřeby pro nějaké služby (aplikace) a sdílí stejnou fyzickou síť (viz obrázek 3.7). Privátním sítím 5G poskytuje diferenciaci služeb například dle rozdílných nároků na úroveň QoS. Network slicing zajistí, že výkon a bezpečnost jedné vrstvy nebude ovlivněna provozem jiných vrstev, což je důležité především pro kritické aplikace [18].

Například jedna vrstva je optimalizována pro aplikace, které vyžadují nízké zpoždění při přenosu, druhá pro vysokou přenosovou rychlost a třetí pro vysoký počet připojených zařízení. Dále některé vrstvy mohou být nakonfigurovány tak, že jejich provoz neopustí privátní síť 5G a naopak jiné vrstvy mají možnost stahovat aktualizace pro software z Internetu a zároveň jsou tak izolovány od kritického provozu [46]. Mezi hlavní výhody konceptu network slicing patří:

- možnost řešit problematiku QoS,
- izolace určitého provozu,
- optimalizace využití zdrojů,
- flexibilita,
- možnost experimentů se sítí v rámci jedné vrstvy.



Obrázek 3.7: Příklad konceptu network slicing pro průmysl [46].

3.6 Definice parametrů pomocí SLA

Service Level Agreement (SLA) je termín označující smlouvu mezi poskytovatelem a uživatelem služby, která má za cíl zajistit spolehlivé poskytování služeb na určité úrovni QoS. SLA určuje očekávání uživatele a odpovědnost poskytovatele služby za nedodržení podmínek, takže pomáhá v případě problému předcházet sporům. ITU-T v doporučení M.3342 [47] definuje základní obsah SLA, ve kterém jsou:

- **Obchodní ujednání** popisující obecné obchodní informace a postupy související se službou. Může obsahovat obecná pravidla, podmínky (porušení služeb a nápravy), informace o fakturaci, postup při ukončení služby a kontaktní údaje.
- **Definice služeb**, která nastiňuje podrobné informace o poskytované službě a její úrovni.
- **Technologická část** poskytující podrobné informace o parametrech QoS, návrhu systému, mechanismech zálohování, upgradech sítě a obsahuje technická doporučení.
- **Reporty QoS** obsahující parametry QoS získané monitorováním služby za účelem vyhodnocení úrovně poskytovaných služeb sjednané ve smlouvě.

Mezi příklady sledovaných parametrů v rámci SLA se typicky řadí maximální, minimální nebo střední hodnoty jako jsou [47]:

- BER (Bit Error Ratio),
- ES (Errored Seconds),
- OI (Outage Intensity),
- SA (Service Availability),
- UAS (Unavailable Seconds),
- zpoždění při přenosu,
- střední doba mezi poruchami,
- střední doba mezi výpadky,
- střední doba opravy,
- střední doba poskytování služby,
- střední doba do obnovení služby.

Mezi základní činnosti pro dodržování SLA se například řadí proaktivní testování sítě, pravidelná údržba, zálohování a dimenzování kapacity. Výpadek poskytované služby může být například zapříčiněn poruchami technologií využívaných v síti, přetížením síťových prvků, poklesem síťových parametrů pod stanovenou mez, kybernetickými útoky nebo nárůstem interferencí a šumem.

4. Rozbor testování síťových parametrů na transportní vrstvě

Motivací pro testování komunikačních sítí může být sledování kvality služby (QoS), kontrolování SLA, dodržování norem, monitorování stavu sítě, předávací řízení, diagnostika poruch či certifikace. Bez testování nelze garantovat a ani hodnotit kvalitu služeb. Při testování je důležité respektovat danou síť a limity vybavení testovacího zařízení. Je často zbytečné příliš zatěžovat síť při testování, protože to nemusí být režim, ve kterém bude síť běžně provozována. Před testováním komunikačních sítí je nutné stanovit:

- cíle testování,
- jaký je očekávaný výstup a mezní parametry sítě (pokud jsou k dispozici),
- jak se testy budou koncipovat (například výběr standardů, metody a kolikrát se budou testy opakovat pro statistickou věrohodnost),
- jaké testovací zařízení se využije.

Pro testování je nutné, aby hardware testovacího zařízení byl výkonnější než testované rozhraní, a tím nedošlo ke zkreslení výsledků. Dále je nutné brát v potaz, zda nějaká jiná aplikace nevyužívá komunikační síť, což by vedlo také ke zkreslení výsledků. Statistické vyhodnocení je způsob, jak odstranit náhodné chyby během testování, proto je vhodné provést několik opakování testů. Také je doporučeno při testování zrušit synchronizaci času s NTP (Network Time Protocol) serverem, aby se při testech neměnil čas, protože nastane problém při zaznamenávání zpoždění při přenosu (zásadní pro testování Wi-Fi a mobilních sítí).

Příklady závěrů z testování sítí jsou funguje/nefunguje, splněno/nesplněno (porovnáno s nějakými mezemi), časový průběh síťových parametrů, výsledky z různých časových úseků dne nebo nějaká statistická hodnota. Při vyhodnocení výsledků je potřeba brát v úvahu to, že:

- různé metody testování (nastavení testů) dávají různé výsledky,
- vzestupný a sestupný přenosový směr se ovlivňuje navzájem,
- zpoždění a ztrátovost paketů degradují přenosovou rychlost sítě,
- sítě se skládají z mnoha různých heterogenních komponent,
- sítě jsou velice rozsáhlé a geograficky rozlehlé,
- sítě se kontinuálně vyvíjí a upravují,
- testovaná síť se v čase mění a páteřní trasy jsou pod živým provozem,
- monitorováním sítí se ovlivňuje jejich chování a parametry,
- neznalost něčeho neznamená, že se to neděje.

Metody testování komunikačních sítí se dělí podle vrstev komunikačního modelu TCP/IP a podle toho, zda se měří za provozu (in service) nebo bez provozu (out-of service) [48]:

- **Aplikační vrstva** – měřiče rychlosti na webových stránkách poskytovatelů a aplikačních serverů.
- **Transportní vrstva** – využití TCP a UDP:
  - využití TCP dle dokumentu RFC 6349,
  - aplikace FlowPing (využití UDP).
- **Síťová vrstva** – využití IP:
  - in service: IP Ping, Trace Route,
  - out-of service: aplikace iPerf nebo FlowPing.
- **Spojová vrstva** – Ethernet:
  - in service: monitorování dle IEEE 802.3ah, .1ag, ITU-T Y.1731 – OAM (Operating and Maintanance),
  - out-of service: test RFC 2544, metoda SAM (Service Activation Methodology) dle ITU-T Y.1564.
- **Fyzická vrstva** – různá dle konkrétní technologie:
  - monitorování blokové chybovosti dle ITU-T G.826 (např. ze zabezpečení CRC – Cyclic Redundancy Check),
  - out-of service: BERT (Bit Error Rate Test) pomocí PRBS (Pseudo Random Binary Sequence) dle ITU-T G.821.

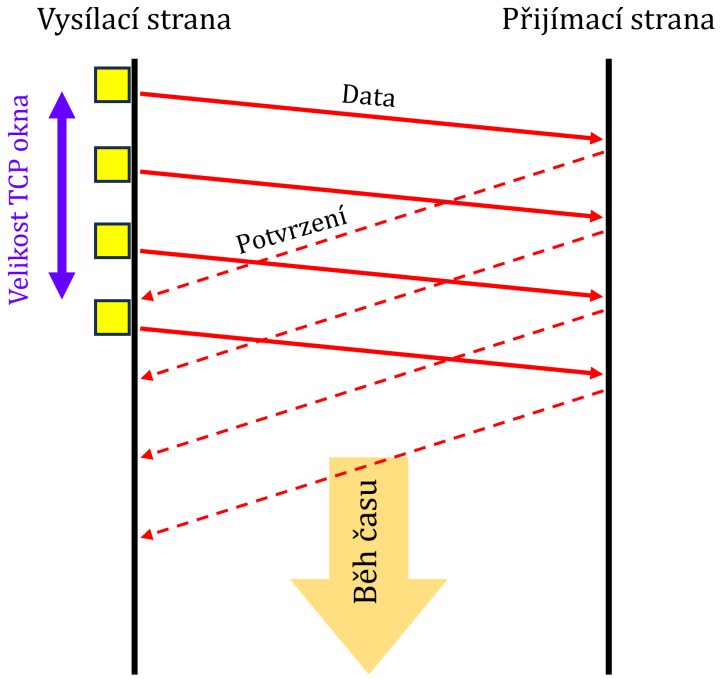
Různé metody testování dávají různé výsledky. Žádná metoda není všespásná, každá má své limity a omezení. Některé metody jsou využívány jako referenční a slouží pro řešení sporů či reklamací. I méně přesné metody jsou dobré z provozních důvodů a mohou dát informaci o tom, že v síti je nějaká degradace. Umístění a konektivita měřicího serveru má vliv na výsledky testování. Typická soustava pro testování zahrnuje [31]:

- **Měřicí server** je využíván jako protistrana pro testy, které jsou spuštěny na měřicím zařízení. Pro případ sestupného směru poskytuje měřicímu zařízení data na vyžádání. Aby se předešlo negativním vlivům na testy, tak musí být pro měřicí server zajištěn vysoký výpočetní výkon, vysoká velikost paměti a vysoká rychlost připojení k Internetu.
- **Měřicí zařízení** je vybaveno nějakým softwarem a měřicími nástroji. Zachycuje získaná data, která následně uchovává v paměti. Pro případ sestupného směru je ve funkci příjemce dat. Je nutné, aby výpočetní a síťový výkon byl dostatečně vysoký kvůli zamezení negativního vlivu na testy.
- **Přenosová trasa** je posloupnost (kaskáda) spojených přenosových uzlů, kde prvním přenosovým uzlem je měřicí zařízení a posledním je měřicí server.

4.1 Testování pomocí TCP a UDP

Pro testování síťových parametrů jsou využívány vlastnosti protokolů transportní vrstvy. TCP (Transmission Control Protocol) je charakteristický tím, že se pokouší alokovat co nejvíce dostupné přenosové kapacity a zohledňuje ostatní toky. Posílá data na základě potvrzování doručení s ohledem na zpoždění a ztrátovost dat při přenosu. Základní princip komunikace pomocí TCP je ten, že vysílací strana čeká s vysíláním dalšího bloku dat dokud nedostane potvrzení o doručení předchozího bloku dat. Existuje případ odesílání bloků dat metodou „okna“, kde velikost TCP okna je objem dat vyslaný bez toho, aniž by bylo doručeno potvrzení od přijímací strany (viz obrázek 4.1). Tedy TCP garantuje spolehlivé doručování dat a opakovaně vysílá data při ztrátě, což snižuje přenosovou rychlost [48].

Dále TCP zajišťuje regulaci datového toku dle stavu sítě. Díky jeho zpětné vazbě dokáže reagovat na stav sítě, což snižuje či zvyšuje přenosovou rychlost pro TCP toky dle potřeby. Na regulaci má negativní vliv zpoždění při přenosu, protože dostat informaci o ztrátovosti dat je vhodné co nejrychleji proto, aby se TCP rychleji adaptoval a neklesala výkonnost sítě. Regulační mechanismus, pro četnost vysílaných paketů, umožňuje měřit přenosovou rychlost. Také se pomocí TCP přirozeně měří zpoždění přenosu ve smyčce.



Obrázek 4.1: Diagram zobrazující odesílání bloků dat metodou „okna“ [48].

UDP (User Datagram Protocol) negarantuje spolehlivé doručování dat, a tím vzniká jejich ztrátovost, takže pomocí tohoto protokolu se detekuje ztrátovost dat (paketů). Je charakteristický tím, že posílá data bez ohledu na stav komunikačního kanálu. Tedy na rozdíl od TCP nemá UDP regulaci na datový tok, a tak je nutné pro testy nastavit nějakou přenosovou rychlost. Mezi metodické nástroje pro testování sítí patří:

- **konstantní toky** (CBR – Constant Bit Rate) – využití UDP (aplikace iPerf),

- **proměnné toky** (VBR – Variable Bit Rate) – využití TCP (aplikace iPerf) nebo emulace požadovaného profilu UDP toků (aplikace FlowPing),
- **kombinace konstantních a proměnných toků** – typický model reálného provozu.

Mezi hlavní zkoumané síťové parametry se řadí:

- přenosová rychlost ve vzestupném směru,
- přenosová rychlost v sestupném směru,
- ztrátovost paketů (PLR – Packet Loss Rate),
- zpoždění ve smyčce (RTT – Round Trip Time),
- kolísání zpoždění.

Přenosová rychlost ve vzestupném směru udává množství přenesených dat za jednotku času (počet bitů za sekundu) ve směru od koncového zařízení směrem k poskytovateli internetové připojení a pro sestupný směr platí směr opačný. Ztrátovost paketů vyjadřuje procento paketů, které nedosáhnou svého cíle. Zpoždění ve smyčce je uplynulá doba mezi odesláním prvního bitu segmentu TCP a příjmem posledního bitu, který potvrzuje segment TCP.

Využitím TCP a UDP při testování lze získat tento soubor síťových parametrů. Pomocí TCP se testuje přenosová rychlost (propustnost sítě) a zpoždění ve smyčce. Pomocí UDP lze validovat ztrátovost paketů. Tato získaná data z testů při využití UDP můžou objasnit například neočekávaně nízkou přenosovou rychlost zjištěnou pomocí TCP. Parametry jako zpoždění a ztrátovost paketů degradují přenosovou rychlost sítě. V rámci QoS je vhodné zkoumat všechny tyto parametry.

4.1.1 Aplikace FlowPing

FlowPing je volně dostupná aplikace, která byla vyvinuta na katedře telekomunikační techniky, FEL, ČVUT v Praze [49]. Umožňuje především testovat, generovat datový provoz a definovat intervaly reportování dat. Využívá UDP nad IPv4 a IPv6 a pracuje v režimu klient/server. Aplikace umožňuje definovat komplexní průběhy pro testování, tedy během testování lze nejen generovat konstantní tok, ale například i zátěž na síť, která se lineárně zvyšuje či snižuje v čase. Dokáže určit zpoždění ve smyčce, jitter a ztrátovost paketů. Dále indikovat pakety mimo pořadí a duplicitní pakety.

Tato aplikace dokáže měnit velikost odesílaných paketů, což je užitečné pro zjištění toho, zda je síť citlivá na tzv. *packet rate* (počet paketů za sekundu). Například při využití velkých paketů dokáže síť přenášet deklarovaný objem dat, ale nedokáže to v situaci, kdy je snížena velikost paketů, a tím je síť zahlcena velkým počtem paketů, nikoliv objemem dat. Je možné realizovat i asymetrické testy, při kterých je možné zmenšit objem dat v jednom z přenosových směrů [50].

Aplikací FlowPing lze vytvořit rostoucí tok (ramp test), a tím otestovat kapacitu sítě. Dochází k detekci zahlcení sítě, kdy je lineárně rostoucí přenosová rychlost a v rámci výstupu testu lze vidět bod, kdy síť zásadním způsobem začne

provoz omezovat (začne růst ztrátovost paketů). Dále lze vytvořit profil přenosové trasy při specifickém zatížení. Například síť je zatížena TCP toky (ty se snaží využít maximum přenosové kapacity) a na pozadí je spuštěna aplikace FlowPing, která slouží k tomu, aby se v nějakých intervalech snímalo zpoždění a ztrátovost paketů. To může být využito pro testování sítě a získání dat, které lze využít pro emulaci sítě [50]. Tuto emulaci lze realizovat například zařízením E-Shaper [51], které dokáže zpožďovat a zahazovat pakety v síti. Tedy emulovat technologie, které byly změřeny pomocí aplikace FlowPing.

4.1.2 Aplikace iPerf a její verze

Aplikace iPerf slouží pro testování vysokorychlostních sítí a dokáže generovat toky pomocí protokolů transportní vrstvy TCP, SCTP či UDP nad IPv4 a IPv6. Jedná se o volně dostupnou aplikaci, která je založena na principu klient/server. Umožňuje měřit například přenosovou rychlost, zpoždění ve smyčce, jitter a ztrátovost paketů. Dokáže testovat sestupným a vzestupným přenosový směr a také testovat pomocí paralelních toků, které jsou nezbytné pro efektivnější vytížení přenosového kanálu [52].

Aplikace iPerf má dvě verze iPerf2 a iPerf3, které jsou vyvíjeny paralelně a mají mezi sebou několik zásadních rozdílů [52, 53]:

- **Režim server** – iPerf2 v režimu server dokáže obsloužit několik klientů. Pro iPerf3 v režimu server platí to, že jedna instance serveru obslouží pouze jednoho klienta, a proto je nutné spouštět více serverů k obsloužení více paralelních klientů.
- **Výkon** – iPerf3 je výkonnější oproti iPerf2, protože iPerf3 plánuje odesílání dat v přesně daných intervalech. iPerf2 vygenerované pakety ihned odesílá na síťovou kartu a nedochází k žádnému plánování odesílání dat.
- **Náročnost** – iPerf2 je spuštěna jako jedna aplikace a každý nový připojený tok je formou vlákna. Naopak u iPerf3 je vše formou procesů, což je nutné brát v úvahu při vytížení operačního systému zařízení a při alokaci paměti pro testování.
- **Počet spojení** – iPerf2 umožňuje vytvořit obousměrný test, a tím v jednom spojení testovat oba přenosové směry. iPerf3 při duálním testu vytváří dvě instance, což má za následek generování přibližně dvakrát více paketů během testování než u iPerf2.
- **Informace o spojení** – Pro iPerf2 jsou dostupné informace jen ze strany klienta, kde je spouštěn test. iPerf3 umožňuje stáhnout i logy ze strany serveru, což poskytuje získat více dat pro následnou analýzu.
- **Parametry** – Režim server u iPerf3 je dynamický, to znamená, že parametry testů, které jsou nastaveny na klientovi, se vykomunikují v rámci serveru na začátku spojení. iPerf2 si nedokáže vyměnit parametry testu při zahájení spojení, a kvůli tomu je nutné nastavovat parametry staticky jak na klientovi, tak na serveru.
- **Výstupní formát** – iPerf2 podporuje formát CSV a iPerf3 podporuje formát JSON.

4.2 Nastavení testu typu TCP

Hlavním cílem testování pomocí TCP je zjištění propustnosti (TCP throughput) sítě a zpoždění přenosu ve smyčce (**RTT** – Round Trip Time). Propustnost je počet úspěšně přenesených bitů za jednotku času, která je testována v určitém bodě na základě přenosu TCP. Zpoždění přenosu ve smyčce určuje rozdíl času od odeslání prvního bitu příjemci po doručení posledního bitu příslušného TCP potvrzení na transportní vrstvě. Dokument RFC 6349 [2] specifikuje parametry a způsob vyhodnocování testování na transportní vrstvě referenčního modelu ISO/OSI. Testy jsou založeny na vlastnostech TCP, tedy na potvrzování doručení datových segmentů a také na tom, že TCP zajišťuje regulaci datového toku dle stavu sítě.

Výsledky testování pomocí TCP jsou blízké vnímání služby uživatelem, jelikož TCP využívá většina aplikací. RFC 6349 [2] nespecifikuje jasný návod, jak naměřit propustnost sítě (dosažitelnou přenosovou rychlost). Problém často nastává v tom, že je zde volnost při nastavování počtu TCP toků a pro rozdílný počet TCP toků jsou získávány různé výsledky. Dále je nutné brát v potaz různé typy algoritmů pro zamezení přetížení sítě (například CUBIC a BBR), u kterých je při stejných parametrech přenosové linky zásadní rozdíl v propustnosti sítě. U algoritmů, které v důsledku ztráty indikují přetížení sítě, má malá ztrátovost paketů (například 0,1 %) znatelný dopad na propustnost sítě při využívání TCP. Důležité je do protokolu z testování uvést nastavení využívaných testů. V dokumentu RFC 6349 jsou definované tyto metriky a parametry [48]:

- minimum TCP **RWND** (Receive Window) – velikost TCP okna v bajtech pro potvrzování přijetí paketů,
- **BDP** (Bandwidth Delay Product) – násobek kapacity datového spoje (v bitech za sekundu) a zpoždění mezi oběma konci spoje (v sekundách),
- **BB** (Bottleneck Bandwidth) – nejnižší hodnota přenosové kapacity celé testované trasy vyjádřená v bitech za sekundu (tzv. *úzké hrdlo*, zjistí se například zkušebními testy),
- **MTU** (Maximum Transmission Unit) – maximální velikost paketu použitelná pro datový spoj (bez nutnosti segmentace),
- Send and Receive Socket Buffers – velikost vysílací a přijímací vyrovnávací paměti.

Dokument RFC 6349 [2] dává základní mantinely pro to, aby se lépe a věrněji měřily síťové různorodé části sítě a rozhraní s ohledem na konkrétní aplikace. Využívá se pro odhad výchozího nastavení TCP okna, které se u aplikace iPerf3 mění. Je důležité, z jaké hodnoty TCP okna se začíná, protože regulační proces je různě rychlý a úspěšný dle nastavení výchozí hodnoty okna. Příliš velké nastavení velikosti TCP okna při testování dynamické sítě zapříčiní to, že bude dlouho trvat adaptace TCP okna a síť nebude rychle reagovat, což zvyšuje ztrátovost paketů, limituje propustnost sítě a může zahlcovat vyrovnávací paměť. Kvůli tomu se nenaměří reálně využitelná přenosová kapacita přípojky.

Čím je menší velikost TCP okna, tím je menší objem dat poslán v čase. Tedy čím je vyšší velikost TCP okna, tím je vyšší přenosová rychlost. Nutné je vzít

v potaz kvalitu sítě při volbě velikosti TCP okna. Optické sítě jsou například charakteristické tím, že jsou spolehlivé, a tak lze využít velikost TCP okna třeba 512 KB. Mobilní sítě naopak mění své síťové parametry dynamicky, a tak je vhodnější využívat menší velikost TCP okna (64 či 128 KB) pro zajištění stabilnějšího spojení. Při časté ztrátovosti je neefektivní znovu posílat data například o velikosti 512 KB. Vhodnou velikost TCP okna lze vypočítat pomocí vzorce

$$\mathrm{RWND} \geq \frac{\mathrm{BDP}}{8}. \tag{4.1}$$

BDP lze spočítat pomocí vzorce

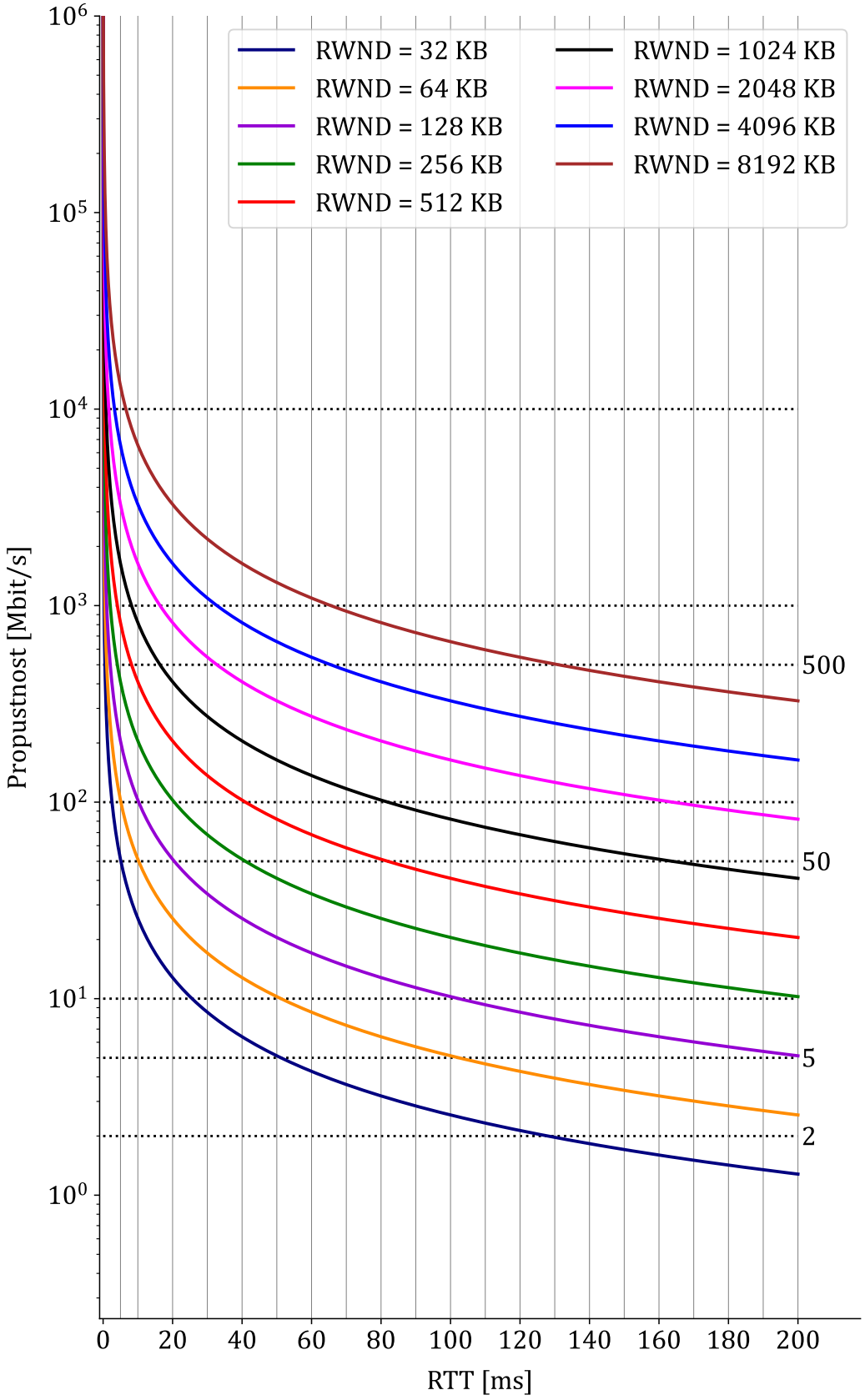
$$\mathrm{BDP} = \mathrm{RTT} \cdot \mathrm{BB}. \tag{4.2}$$

S velikostí TCP okna souvisí i počet TCP toků. Pro určitou velikost TCP okna se při zvyšujícím se zpoždění přenosu ve smyčce (RTT) redukuje propustnost. Z obrázku 4.2 je patrné, že například při využití jednoho TCP toku nelze u velikosti TCP okna 512 KB a při zpoždění ve smyčce (RTT) 100 ms dosáhnout přenosové rychlosti 50 Mbit/s. Kvůli tomu, aby se dosáhlo co nejvěrohodnější pokrytí celé kapacity přenosové trasy a vyplnila se maximální přenosová kapacita, se využívá více TCP toků. Stanovení vhodného počtu TCP toků lze pomocí vzorce

$$N \geq \frac{\mathrm{BDP}}{8 \cdot \mathrm{RWND}}, \tag{4.3}$$

kde N je počet TCP toků (zaokrouhleno na nejbližší vyšší celé číslo) [54]. Čím vyšší počet TCP toků je nastaven (navzájem si konkurují), tím bude využívána menší velikost TCP okna při přenosu. Díky tomu je rychlejší reakce na změny v síti. Při nastavení zbytečně vysokého počtu TCP toků se přenosový kanál přetěžuje, a tím může nastat pokles v přenosové rychlosti. Tedy naměří se přenosová rychlost nižší, než kdyby tam bylo méně TCP toků. Obecně je doporučeno nejdříve provést zkušební testy s různým nastavením a sledovat reakci zkoumané sítě.

Propustnost (dosažitelná přenosová rychlost) na transportní vrstvě je nižší oproti síťové, spojové a fyzické vrstvě kvůli přidanému záhlaví paketům. Další příčinou snížení propustnosti tvoří nedoručené pakety, které TCP vyžaduje opakovaně přeposlat a zároveň se uplatňují jeho regulační mechanismy (ochrana sítě před přetížením), při kterých dochází k pozvolnému náběhu při sestavení spojení a zpomalování komunikace při nárůstu ztrátovosti [48].



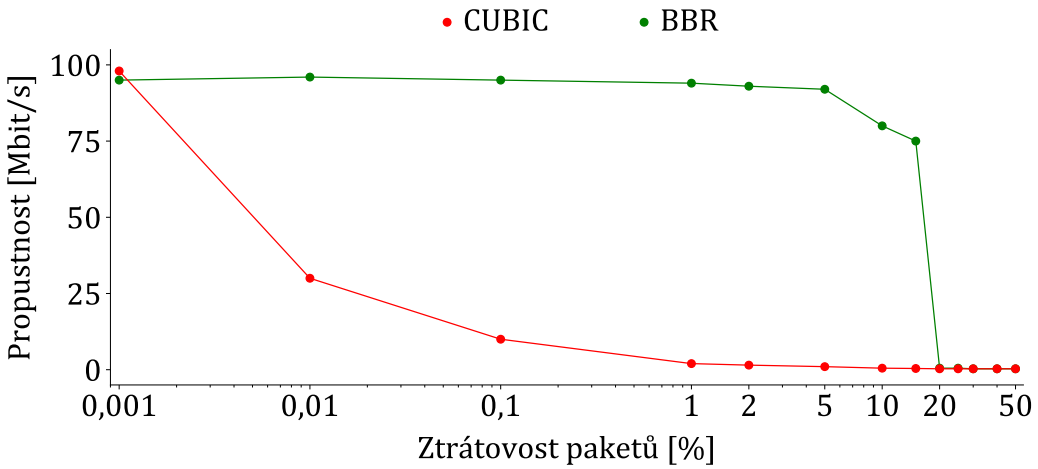
Obrázek 4.2: Maximální dosažitelná propustnost u TCP spojení.

4.2.1 Algoritmy CUBIC a BBR

TCP může například využívat algoritmy CUBIC a BBR (Bottleneck Bandwidth and Round-trip) pro zamezení přetížení sítě, které negativně ovlivňuje síťové parametry a může blokovat nová spojení. Algoritmy jsou odpovědné za to, že když mají dostupnou přenosovou kapacitu, tak zintenzivní množství dat vstupujících do přenosového kanálu. Pokud dostupnou přenosovou kapacitu nemají, tak množství dat sníží. Tyto algoritmy předcházejí zahlcení sítě jinými způsoby. Algoritmus CUBIC zvyšuje přenosovou rychlost a pokud detekuje ztrátu paketů, tak sníží přenosovou rychlost. Po následném obnovení ztracených paketů roste přenosová rychlost přes kubickou funkci. Například u většiny distribucí Linux je nastaven jako výchozí algoritmus CUBIC [55].

Algoritmus BBR zvyšuje přenosovou rychlost, jestliže je plná vyrovnávací paměť. Poté dochází ke snížení přenosové rychlosti a během toho je čas pro obnovení ztracených paketů, které byly ztraceny při přenosu se zvýšenou přenosovou rychlostí. Například při využívání YouTube je nasazován algoritmus BBR. Hlavní rozdíl mezi algoritmy CUBIC a BBR je ten, že BBR delší dobu ignoruje narůstající ztrátovost paketů [56]. Tedy algoritmus CUBIC oproti algoritmu BBR dříve sníží přenosovou rychlost jako reakci na narůstající ztrátovost paketů (viz obrázek 4.3, na kterém je zobrazen příklad, kde BB = 100 Mbit/s, RTT = 100 ms a byl využit jeden TCP tok).

Obecně platí, že při využití algoritmu CUBIC je dosahováno vyšší přenosové rychlosti, pokud je hodnota BDP malá a je k dispozici velká vyrovnávací paměť. Naopak při využití algoritmu BBR je dosahováno vyšší přenosové rychlosti při vysoké hodnotě BDP a je k dispozici málo vyrovnávací paměti. Algoritmus BBR může zapříčinit mnoho retransmisí paketů oproti algoritmu CUBIC, protože kvůli malé vyrovnávací paměti může docházet k častým retransmisím paketů. Pokud je nějaká aplikace citlivá na ztrátovost paketů, tak algoritmus BBR není vhodný. Algoritmus CUBIC je vhodný pro sítě s velkým zpožděním paketů. Naopak algoritmus BBR je vhodný pro sítě s vysokou přenosovou rychlostí a s nízkým zpožděním při přenosu [56].



Obrázek 4.3: Příklad reakce algoritmů CUBIC a BBR na ztrátovost paketů, kde BB = 100 Mbit/s, RTT = 100 ms a byl využit 1 TCP tok [57].

4.3 Platforma F-Tester

Platforma F-Tester poskytuje ověření výkonnosti a spolehlivosti komunikačních sítí založených na rodině protokolů TCP/IP. F-Tester 5G umožňuje testování mobilních sítí například i za jízdy. Několik verzí zařízení F-Tester (viz obrázek 4.4 a 4.5) bylo vyvinuto na katedře telekomunikační techniky, FEL, ČVUT v Praze. Lze vytvořit scénáře z testů s různým datovým profilem generovaných dat. Výsledky testování jsou vyhodnoceny korelovanými časovými průběhy odezvy například v podobě propustnosti (přenosové rychlosti), zpoždění paketů ve smyčce a ztrátovosti paketů při přenosu. Dále je i možné měřit rádiové parametry RSSI, RSRQ, RSRP, SINR a SNR [58].

Je možné provádět krátkodobé nebo dlouhodobé testování. Krátkodobé testování slouží pro přehledové ověření funkčnosti a zjištění mezních parametrů. Dlouhodobé testování umožňuje získání dat v horizontu hodin, dnů, týdnů, měsíců a také umožňuje testování stability komunikace. F-Tester zobrazí výsledky testů v tabulkách a grafech. Dále je možné tyto výsledky vygenerovat ve formátu PDF, JSON nebo CSV. Typy testů, ze kterých se tvoří scénáře pro testování komunikačních sítí jsou [58]:

- Testy využívající **TCP** (iPerf3):
  - testování propustnosti datového toku v sestupném nebo vzestupném přenosovém směru,
  - zjištění zpoždění paketů ve smyčce a stability spojení,
  - konfigurovatelné parametry jako je například počet paralelních TCP toků, velikost TCP okna a MSS (Maximum Segment Size),
  - možnost nastavení velikosti TCP okna staticky nebo dynamicky,
  - volba typu TCP algoritmu Reno, CUBIC, BBR a Hybla.
- Testy využívající **UDP** (iPerf3, FlowPing):
  - tvorba toku s konstantní či proměnnou přenosovou rychlostí,
  - zjištění mezí propustnosti sítě,
  - zjištění stability při konstantním toku,
  - vyhodnocení zpoždění ve smyčce,
  - validace ztrátovosti paketů.

Obrázek 4.4: F-Tester NGA [59].

Obrázek 4.5: F-Tester 5G [60].

5. Návrh metodiky pro testování privátních sítí 5G

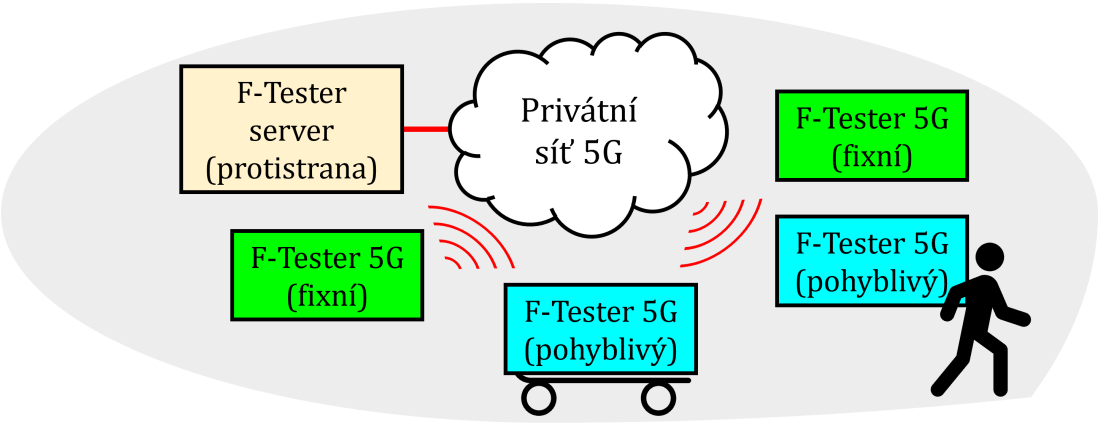
Metodika pro testování privátních sítí 5G pomocí platformy F-Tester popisuje postupy pro zjištění síťových parametrů (vhodné pro ověřování parametrů QoS a SLA) a chování sítě pro případy, mezi které patří:

- testování maximální propustnosti (dosažitelné přenosové rychlosti) sítě,
- zatěžování sítě konstantními či proměnnými toky,
- testování konkurence mezi toky v síti,
- emulování určitého síťového provozu, kterému je síť běžně v průmyslu vystavována a zjistit, zda síť dokáže poskytnou podmínky, které služba vyžaduje.

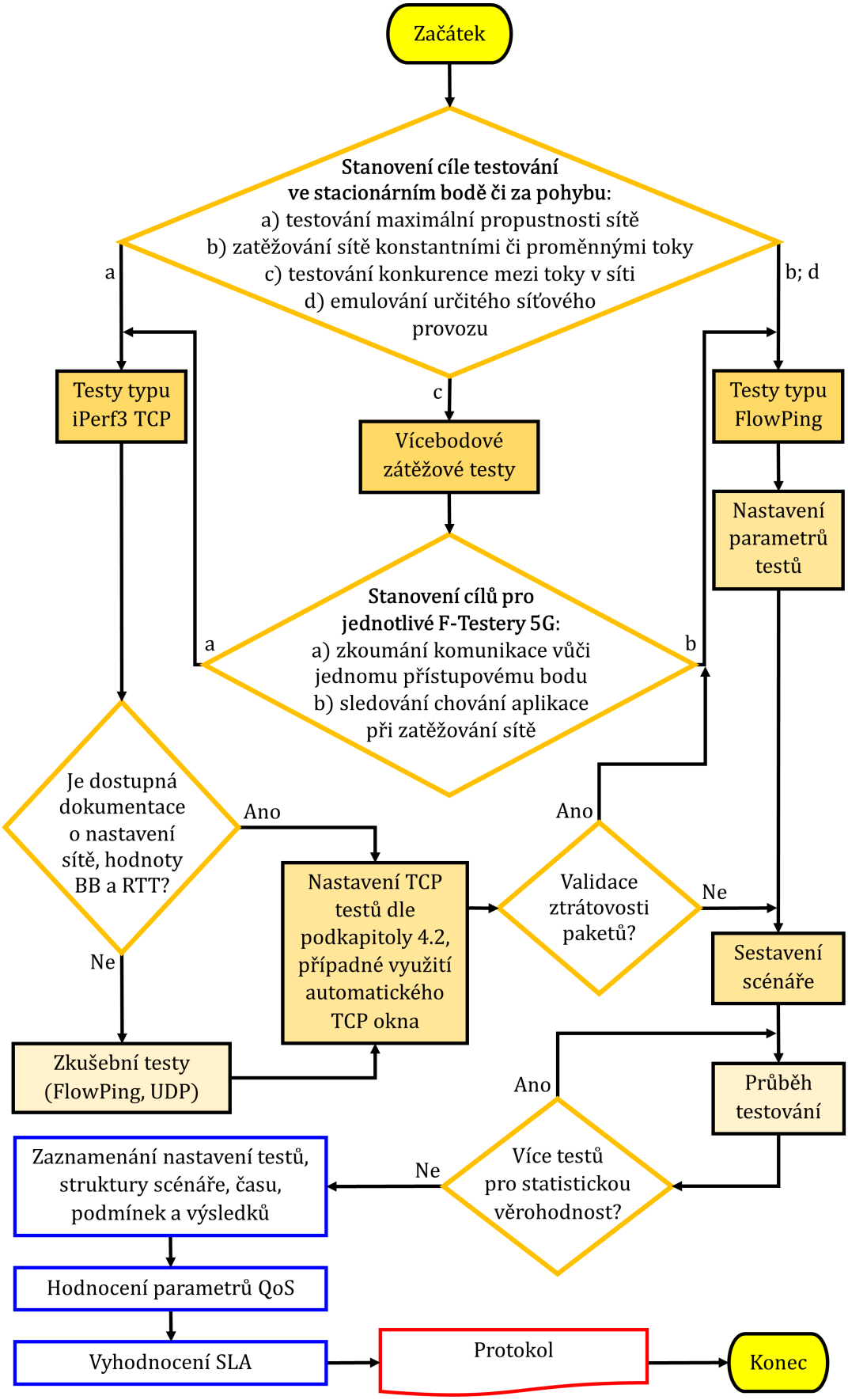
Platforma F-Tester (viz podkapitola 4.3) umožňuje vygenerovat soubor CSV, který obsahuje parametry v závislosti na čase jako je propustnost, RTT, PLR, jitter, RSSI, RSRQ, RSRP, SINR, SNR, RWND, CWND, režim MIMO, využité kmitočtové pásmo, IMEI, ID buňky, informace o využívané modulaci a kanálu.

Metodika bere v úvahu různé nastavení privátních sítí 5G. Pro scénáře testování jsou využívány testy typu FlowPing (využití UDP), iPerf3 UDP a iPerf3 TCP, které jsou teoreticky popsané v podkapitole 4.1. Nastavení testů typu iPerf3 TCP vychází z dokumentu RFC 6349 [2]. Obrázek 5.2 zobrazuje vývojový diagram popisující kroky této metodiky. Kapitola 4 obsahuje problematiku testování komunikačních sítí, a to, co je nutné brát v úvahu při testování a nastavování jednotlivých testů, ze kterých se skládají scénáře testování.

Obrázek 5.1 znázorňuje příklad schématu zapojení soupravy pro testování. Zde je do privátní sítě 5G připojeno několik F-Testerů 5G (fixní a pohyblivé, pro stacionární testování a testování za pohybu) a F-Tester v režimu server, který slouží jako protistrana pro F-Testery 5G. Nutné je využívat protistranu pro testování s dostatečnou kapacitou a výkonem, aby zde nebylo vytvořeno tzv. *úzké hrdlo* a nedocházelo ke zkreslení testování. F-Testerům 5G je nutné přidělit IP adresy a SIM karty pro privátní síť 5G.



Obrázek 5.1: Příklad zapojení soupravy pro testování privátní sítě 5G.

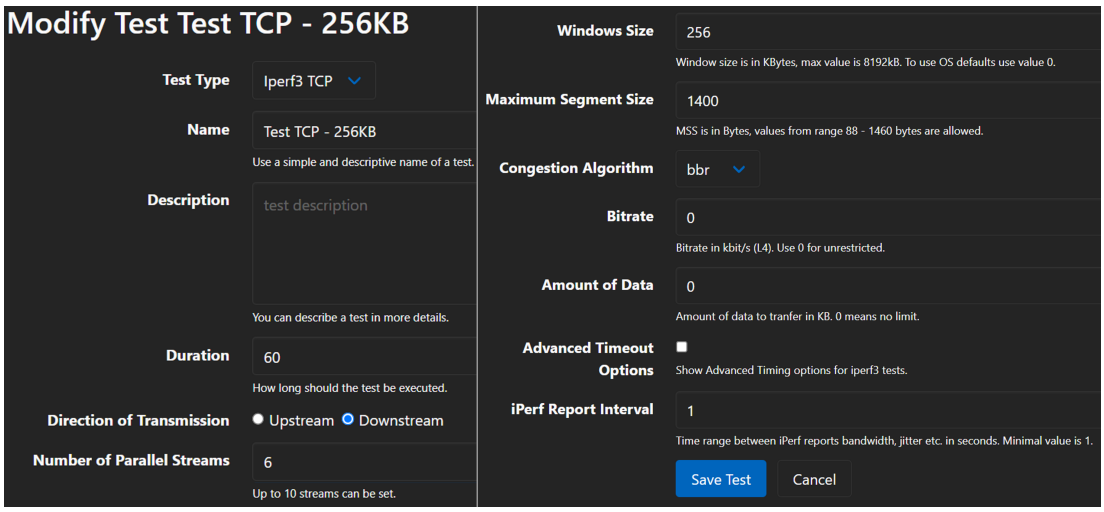


Obrázek 5.2: Vývojový diagram metodiky testování sítí platformou F-Tester.

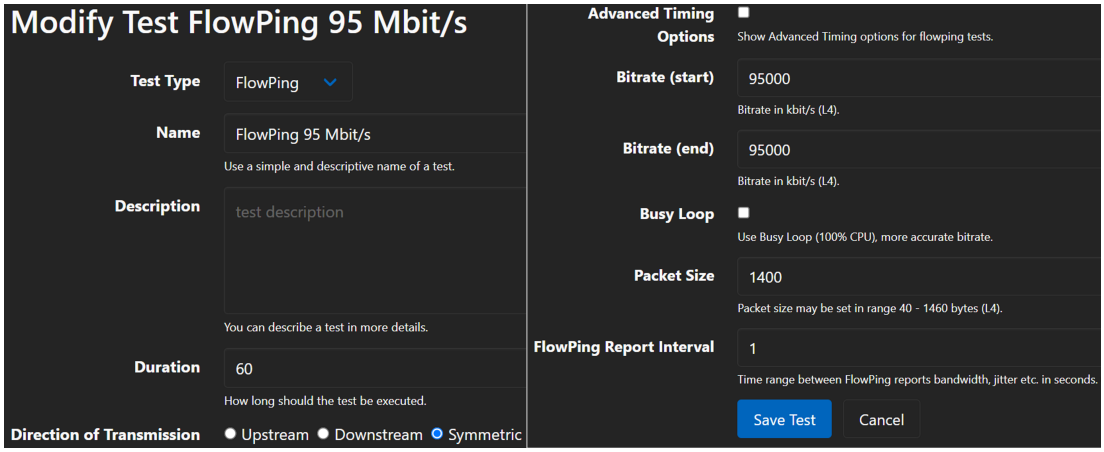
Pro testování ve stacionárním bodě je doporučena délka jednotlivých testů tak, aby byly zahrnuty všechny aspekty, které by testování mohly ovlivnit. Obecně platí, že se má testovat „do ustálení“ a ideálně opakovaně během dne s dostatečnou časovou a provozní diverzitou pro statistickou věrohodnost. Pro stanovení délky testování je nutné brát v potaz zpoždění při přenosu a případně velikost TCP okna (množství přenesených dat bez potvrzení). V privátních sítích je zpoždění maximálně stovky milisekund, takže například test trvající 1 minutu je vypovídající, avšak pro sítě se zpožděním 1 sekunda je tato doba krátká pro vypovídající test. Protokol z testování sítě by měl obsahovat:

- cíle testování,
- seznam použitých nástrojů,
- hodnoty použité pro nastavení jednotlivých testů,
- časové údaje,
- místo testování,
- chronologii testů,
- počet opakování,
- zjištěné síťové parametry pro oba přenosové směry,
- grafy,
- statistické zpracování,
- porovnání s tolerančními mezemi (QoS, SLA) a závěr.

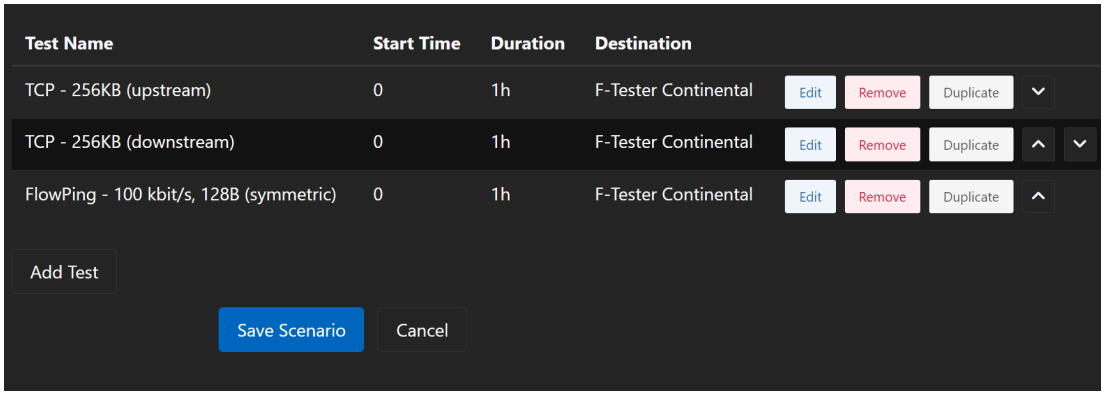
Obrázky 5.3 a 5.4 zobrazují uživatelské rozhraní, ve kterém se nastavují testy a obrázek 5.5 ukazuje uživatelské rozhraní pro sestavení scénáře z definovaných testů. Obrázek 5.6 nastiňuje chronologicky nezbytné kroky pro testování pomocí platformy F-Tester.



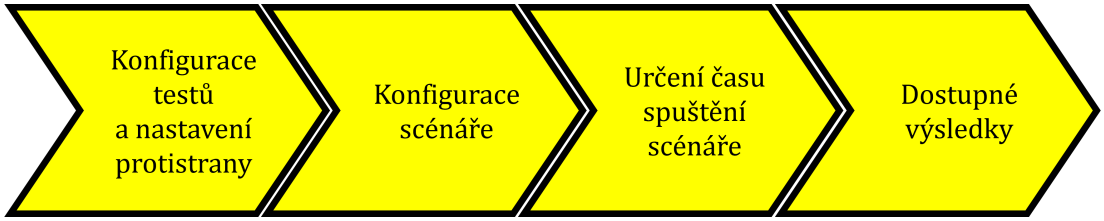
Obrázek 5.3: Uživatelské rozhraní pro nastavení testu typu iPerf3 TCP.



Obrázek 5.4: Uživatelské rozhraní pro nastavení testu typu FlowPing.



Obrázek 5.5: Uživatelské rozhraní pro sestavení scénáře testování.



Obrázek 5.6: Sekvence kroků pro testování pomocí platformy F-Tester.

5.1 Využití testů typu FlowPing

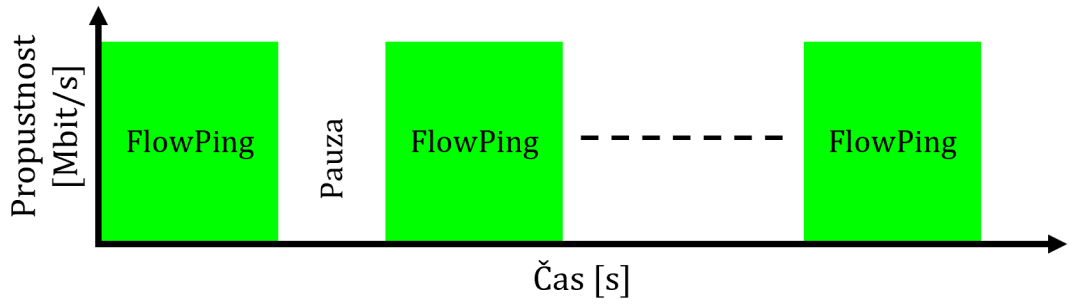
Aplikace FlowPing (viz podkapitola 4.1.1), která využívá UDP, slouží pro tvorbu toků emulující nějaké služby (zátěžové testy) a pro validaci ztrátovosti paketů. Tedy lze vytvořit konstantní nebo proměnlivý tok v čase emulující nějakou aplikaci využívanou v *Průmyslu 4.0* a sledovat reakci sítě. F-Tester pro test typu FlowPing umožňuje nastavit délku testu, přenosový směr, velikost paketů (do 1460 B) a nějakou konstantní přenosovou rychlost nebo nastavit počáteční hodnotu přenosové rychlosti, která se během testu bude lineárně zvyšovat do nastavené konečné hodnoty. Z těchto testů lze sestavit určitý scénář pro testování, který se dle stanoveného času spustí. Dále je nutné vzít v potaz možné hardwarové omezení, které může limitovat využití FlowPingu například do 250 Mbit/s u platformy PC Engines APU3.

Pomocí aplikace FlowPing lze modelovat testy s:

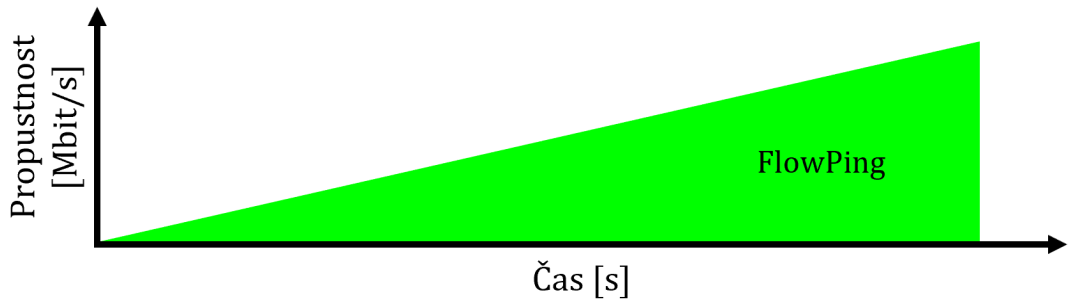
- konstantním tokem,
- dávkovým tokem (burst test),
- rostoucím tokem (ramp test).

Využíváním konstantních toků lze emulovat signály z kamer či stream dat například pro brýle, které budou sloužit pracovníkům pro virtuální realitu, kde mohou absolvovat nácvik různých činností. Dále lze konstantní tok přidat do scénáře pro validaci ztrátovosti paketů při využívání testu typu iPerf3 TCP. Testy s dávkovým tokem (viz obrázek 5.7) mají za úkol emulovat situace, při kterých může nastat, že v jeden okamžik dojde nárazově k vysílání velkého množství dat ze senzorů nebo dalších zařízeních (reakce sítě na mnoho vyslaných dat v jeden okamžik).

Testy s rostoucím tokem (viz obrázek 5.8) emulují lineární nárůst zatížení sítě v čase. Slouží k ověření mezí propustnosti. Tedy pro odhalení meze zatížení sítě, při které je stále minimální zpoždění a ztrátovost paketů. To je důležité například pro řízení robotů, aby reagovali co nejrychleji na povely. Dále tyto testy mohou sloužit pro zkušební testy (pokud nejsou dostupné informace o nastavení síti) pro zjištění parametrů, které jsou nutné pro nastavení testu typu iPerf3 TCP.



Obrázek 5.7: Průběh dávkového toku v čase.



Obrázek 5.8: Průběh rostoucího toku v čase.

Také lze pomocí aplikace FlowPing najít mez pro zátěž v síti, kdy je ještě plynulý například video stream do brýlí pro virtuální realitu. Znalost této meze předejde tomu, aby kvalita této služby při provozu byla pro uživatele frustrující. Aplikací FlowPing se vytvoří určitá zátěž na zkoumanou síť a současně se sleduje, jakou má tato zátěž vliv na kvalitu video streamu do těchto brýlí. Na základě těchto testů se následně vypracuje doporučení pro využívání sítě nebo se zváží navýšení kapacity sítě dle potřeb nějaké aplikace či na druhou stranu úpravu rozlišení, video kodeku a kompresního poměru pro snížení datového toku.

5.2 Využití testů typu iPerf3 TCP

TCP je charakteristický tím, že se pokouší alokovat co nejvíce dostupné přenosové kapacity. Tedy tyto testy reprezentují typicky přenos většího množství dat, například stahování souborů. Využití TCP při testování slouží především pro zjištění maximální propustnosti sítě a hodnoty RTT (viz podkapitola 4.1). Platforma F-Tester umožňuje u testu typu iPerf3 TCP nastavit délku testu, přenosový směr (vzestupný či sestupný směr), počet paralelních TCP toků (až 10 toků), velikost TCP okna (do 8192 KB), MSS (do 1460 B), typ algoritmu pro zamezení přetížení sítě (CUBIC, Reno, BBR a Hybla) a případné limity na přenosovou rychlost a počet přenesených dat. Z těchto testů lze sestavit určitý scénář, který se dle stanoveného času spustí.

U testu typu TCP je klíčové nastavit správně velikost TCP okna a počet TCP toků (postup obsahuje kapitola 4.2), aby nedošlo ke zkreslení výsledků testování. Je nutné vzít v potaz, že teoretická maximální propustnost spojení při použití TCP je dána rovnicí

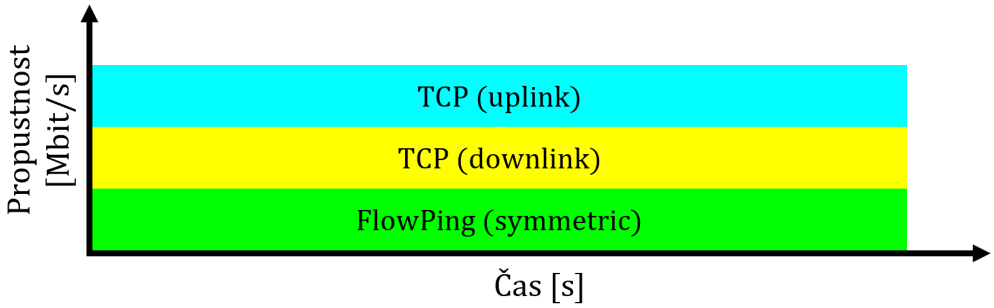
$$\mathrm{TP}_{\mathrm{TCP}} = \frac{8 \cdot \mathrm{WS}}{\mathrm{RTT}}, \tag{5.1}$$

kde WS je velikost TCP okna (množství dat, které jsou do sítě poslána aniž by bylo vyžadováno potvrzení od protější strany) v bajtech na straně vysílače a RTT (Round Trip Time) je zpoždění ve smyčce, tedy časový interval, který uplyne od vysílání segmentu do příjmu jeho potvrzení. Obrázek 4.2 zobrazuje omezení propustnosti (dosažitelná přenosová rychlost) v závislosti na RTT a RWND. Dále je nutné vzít v potaz velikost vysílacího okna CWND (Congestion Window), která značí, že pokud se nemění dynamicky čase, tak limitem může být nastavení testu, přidělená paměť, nedostatečný výkon či nějaký problém u protistrany pro testování, kdy není schopná data přijímat. Pokud se hodnota CWND v průběhu testu mění dynamicky, tak to indikuje, že tzv. *úzkým hrdlem* je testovaná síť, což je vyhovující stav pro testování, aby nedošlo ke zkreslení výsledků. Navýšení propustnosti TCP spojení lze dosáhnout nastavením vyššího počtu paralelních TCP toků v testu dle rovnice 4.3. Výsledná propustnost je sumace všech toků. Například je to nutné vzít v potaz při využívání kmitočtového pásma 26 GHz (šířka kanálu 200 MHz), u kterého je značný nárůst přenosové rychlosti.

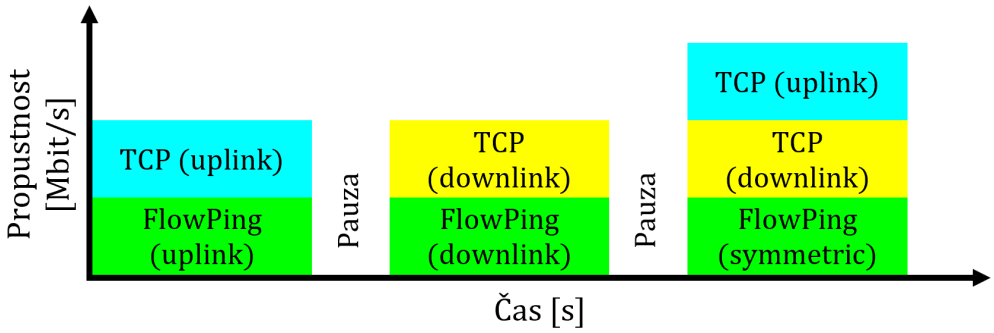
Dále u testu typu TCP je nutné věnovat pozornost volbě algoritmu pro zamezení přetížení sítě například kvůli reakci těchto algoritmů na ztrátovost paketů (viz podkapitola 4.2.1). To znamená, že i malá ztráta paketů (například 0,1 %) má znatelný dopad na propustnost TCP u algoritmů, které kvůli ztrátě detekují zahlcení sítě. Vhodné nastavení parametrů testu typu iPerf3 TCP vychází z toho, že jsou známé nastavené parametry sítě buď z dokumentace nebo ze zkušebních

testů. Důležité je, aby se zapsalo do protokolu nastavení testů TCP a všechny podmínky, za kterých bylo testování vykonáváno. To, co je nutné brát v úvahu při vyhodnocování výsledků testování popisuje kapitola 4.

Obrázek 5.9 zobrazuje scénář složený ze tří testů. Dva jsou typu iPerf3 TCP, které testují přenosový směr vzestupný (uplink) a sestupný (downlink). Třetí test je typu FlowPing, který má za cíl validovat ztrátovost paketů. Tento scénář, který je aplikovatelný pro stacionární testování a testování za pohybu. Je především vhodný pro zjištění maximální propustnosti sítě. Získané hodnoty při zatížení obou přenosových směrů zároveň jsou více relevantní, protože je síť více vytížena a u TCP spojení se vzestupný i sestupný směr navzájem ovlivňují. Je možné i sestavit komplexnější scénář (tzv. *dávkový režim*), při kterém se v určitý čas bude testovat pouze vzestupný směr a po krátké pauze, pro stabilizaci systému, sestupný směr. Po další pauze se testují oba směry současně (viz obrázek 5.10).



Obrázek 5.9: Scénář využívající TCP a aplikaci FlowPing.



Obrázek 5.10: Komplexní scénář využívající TCP a aplikaci FlowPing.

5.2.1 Automatické nastavování velikosti TCP okna

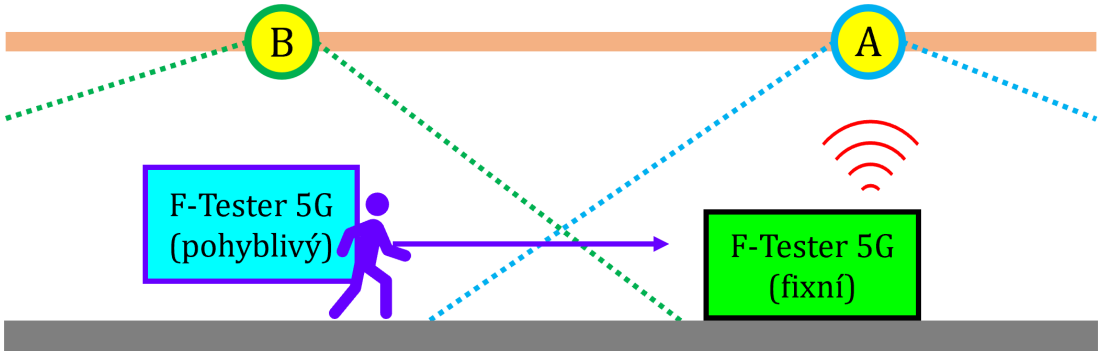
Platforma F-Tester má možnost automatického adaptivního nastavování velikosti TCP okna dle velikosti dostupné paměti, která je zjištěna ještě před spuštěním daného testu. Pro využití této možnosti se při nastavení testu typu iPerf3 TCP zadá u velikosti TCP okna hodnota 0 KB. Při využívání automatického adaptivní nastavování velikosti TCP okna je nutné vzít v potaz to, že pokud dojde ke ztrátovosti paketů při využívání velkého TCP okna, tak dojde k opětovnému poslání celého bloku dat o velikosti stanoveného TCP okna, a tím se snižuje

propustnost sítě. To znamená, že při časté ztrátovosti paketů je neefektivní znovu posílat data například o velikosti 1024 KB. Dále při využívání velkého TCP okna bude dlouho trvat jeho adaptace a včas se nezjistí, že se zvyšuje ztrátovost paketů, a tím dojde k limitaci propustnosti sítě.

Zařadit tuto možnost pro testování maximální propustnosti privátní sítě 5G v průmyslu je vhodné, protože se jedná o stabilní prostředí a o spolehlivou síť. Pro nestabilní prostředí je vhodné využívat pevně nastavené nižší TCP okno (například 64 KB či 128 KB) a využívat vyšší počet TCP toků pro nezkreslené testování. Dále je při využívání automatického nastavování velikosti TCP okna nutné počítat s tím, že hodnota RTT (časový interval, který uplyne od vysílání segmentu do příjmu jeho potvrzení) se dynamicky mění kvůli častým změnám velikosti TCP okna (množství dat poslaných do sítě bez potvrzení), které nemá v testu stanovenou maximální hodnotu.

5.3 Vícebodové zátěžové testy

Vícebodové zátěžové testy pomocí několika F-testerů 5G jsou určeny ke zkoumání, jakým způsobem si toky v privátní síti 5G konkurují a jak si plánovač základnové stanice poradí se změnami požadavků jednotlivých terminálů. Pro vícebodové testy je vhodné (doporučení vyplývající z testování privátní sítě 5G popsané v kapitole 6) mít v síti pro služby nastavené QoS parametry, aby plánovač nepřiděloval přenosovou kapacitu nepředvídatelně. Mezi testy pro sdílené toky se řadí sledování komunikace vůči jednomu přístupovému bodu. Například jeden F-Tester 5G (fixní) bude generovat TCP toky, které budou maximálně zatěžovat přístupový bod A. Druhý F-Tester 5G (pohyblivý) bude generovat také TCP toky maximálně zatěžující jiný přístupový bod B a v průběhu se přemístí do místa, ve kterém se připojí k přístupovému bodu A. Tak bude zkoumáno rozdělení kapacity přístupového bodu (jeho přizpůsobení) pro dva F-Testery 5G generující TCP toky (viz obrázek 5.11).



Obrázek 5.11: Příklad průběhu vícebodových zátěžových testů.

Dále například na jednom F-testeru 5G je spuštěn test typu FlowPing (generuje UDP toky) s rostoucím tokem a na druhém F-testeru 5G je spuštěn test typu iPerf3 TCP (reprezentace nějaké aplikace využívané v průmyslu). UDP toky jsou dominantní v rámci zabírání kapacity nad TCP toky. To znamená, že TCP toky se přizpůsobují stavu sítě. Tím bude zkoumána degradace kvality aplikace využívané v průmyslu způsobenou „agresivnějším“ UDP tokem.

6. Testování privátní sítě 5G ve společnosti Continental

Společnost *Continental Automotive Czech Republic s.r.o.* v Brandýse nad Labem provozuje privátní síť 5G implementovanou společností *T-mobile Czech Republic a.s.* Signál zatím pokrývá 5000 m^2 výrobní plochy, což poskytuje osm přístupových bodů (Radio Dots, viz obrázek 6.1). Do sítě bude připojeno více než tisíc zařízení a senzorů [61]. Systém Radio Dots od společnosti *Ericsson* podporuje 4×4 MIMO, carrier aggregation, network slicing, geolokaci, modulaci 256 QAM (Quadrature Amplitude Modulation), TDD (Time Division Duplex) a FDD (Frequency Division Duplex) [62]. Zařízení IRU (Indoor Radio Unit, viz obrázek 6.2) je součástí Radio Dots systému. Jedná se o jednotku, která agreguje signály a napájí zařízení Radio Dots (lze připojit 8 až 16 Radio Dots) [63]. Deklarované nastavené hodnoty parametrů privátní sítě 5G jsou:

- kmitočtové pásmo 3,5 GHz,
- šířka pásma 60 MHz,
- přenosová rychlost ve vzestupném směru (uplink) 200 Mbit/s,
- přenosová rychlost v sestupném směru (downlink) 550 Mbit/s,
- zpoždění v jednom směru přenosu 10 ms.

Obrázek 6.1: Radio Dot [62].

Obrázek 6.2: Indoor Radio Unit [63].

Ve společnosti *Continental Automotive* byla a je využívána bezdrátová technologie Wi-Fi, která bude s privátní sítí 5G koexistovat. V první fázi je privátní síť 5G nasazena jako experimentální pro získávání dat z výrobních strojů a pro řešení s využitím rozšířené reality pro zaškolování nových zaměstnanců. V další fázi tato síť pomůže s využíváním autonomních vozíků a strojového vidění [61].

Vlastnosti privátní sítě 5G jsou klíčové pro přechod na plně digitální firmu v rámci konceptu *Průmysl 4.0*. Cílem společnosti *Continental Automotive* je postupně rozšiřovat privátní síť 5G do dalších výrobních hal a připojovat další roboty a senzory tak, aby byly maximálně využity vlastnosti této sítě. Tím bude efektivnější i bezpečnější výroba, větší přehled o celém výrobním řetězci a omezí se odstávky výrobních linek z důvodu nečekaných poruch zařízení díky prediktivní údržbě.

Nízké zpoždění při přenosu umožňuje práci v prostředí rozšířené nebo virtuální reality, což zajistí úsporu nákladů a času při školení zaměstnanců. Prostřednictvím virtuální reality lze bez rizika absolvovat nácvik různých činností v oblastech, ve kterých by v reálném světě mělo nějaké pochybení nepříznivé následky [64]. Další příklady možností využití privátní sítě 5G v *Průmyslu 4.0* obsahuje podkapitola 2.3.

Testování parametrů privátní sítě 5G v prostředí *Průmyslu 4.0* je klíčovým krokem k ověření spolehlivého a efektivního provozu. Tedy zjišťovat limity sítě, aby následně během provozu bylo možné maximálně těžit z vlastností této sítě, které jsou důležité pro průmyslové aplikace. Dále je vhodné prověřovat bezpečnostní opatření, šifrování, řízení přístupu pro ochranu citlivých dat a integrity komunikace v rámci privátní sítě 5G. Mezi hlavní zkoumané prvky privátní sítě 5G se řadí:

- přenosová rychlost (propustnost sítě),
- zpoždění při přenosu,
- ztrátovost paketů při přenosu,
- parametry signálu,
- pokrytí výrobní haly signálem.

6.1 Prvotní testy privátní sítě 5G

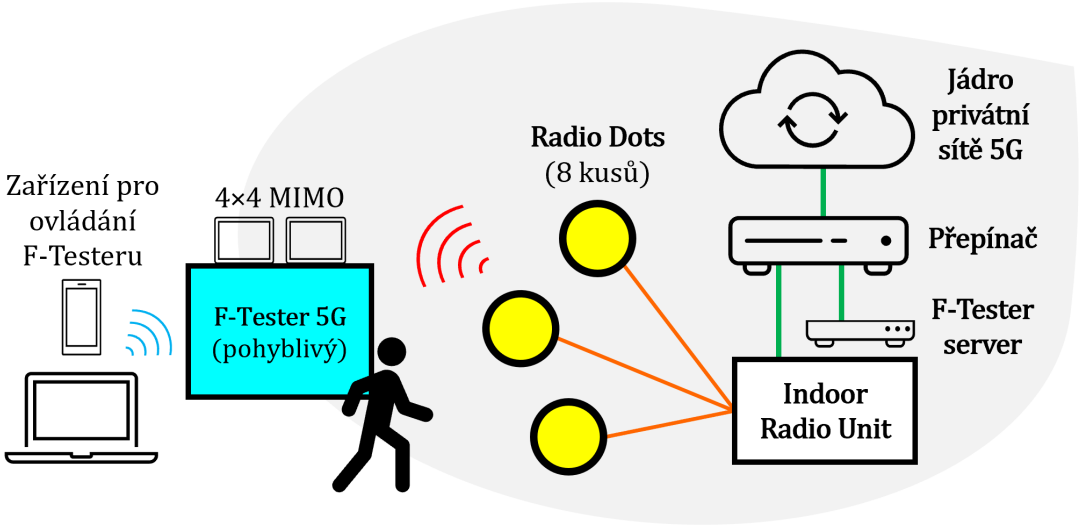
Prvotní testy ve společnosti *Continental Automotive* v Brandýse nad Labem proběhly v pátek 10. 11. 2023. Měly za cíl zjistit řádové hodnoty síťových parametrů (na transportní vrstvě) privátní sítě 5G. Na základě těchto zjištěných hodnot byly nastaveny testy, ze kterých se skládaly scénáře pro pokročilejší testování (viz podkapitola 6.2).

6.1.1 Zapojení a použité nástroje pro prvotní testy

Na obrázku 6.3 je zobrazeno propojení nástrojů pro prvotní testování do privátní sítě 5G. Pro testování síťových parametrů této sítě byly použity tyto nástroje:

- F-Tester 5G v batohu (pohyblivý),
- F-Tester v režimu server jako protistrana pro testy (rozhraní 1GE),
- SIM karta od společnosti *Ericsson*,
- 4×4 MIMO antény,
- notebook a mobilní telefon.

V F-testeru 5G (pohyblivý) byla umístěna SIM karta od společnosti *Ericsson*. F-Tester v režimu server byl zapojen do infrastruktury a sloužil jako protistrana pro testy. Obrázek 6.4 zobrazuje F-Tester v režimu server spolu s IRU jednotkou a obrázek 6.5 zobrazuje Radio Dot. Mobilní telefon a notebook se využili pro obsluhu F-Testerů.



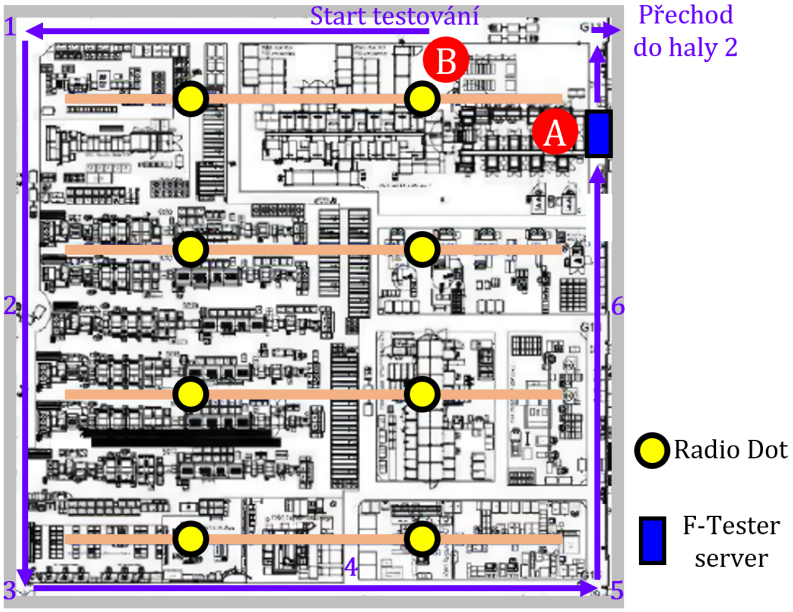
Obrázek 6.3: Schéma zapojení prvotního testování privátní sítě 5G.

Obrázek 6.4: F-Tester server (protistrana pro testy) položený na IRU jednotce.

Obrázek 6.5: Radio Dot (vlevo) umístěný vedle Wi-Fi modemu (vpravo).

6.1.2 Realizace a výsledky prvotních testů

V rámci prvotních testů proběhly testy za pohybu a stacionární testy, při kterých byl využit F-Tester 5G (pohyblivý, umístěn v batohu) a jeden F-Tester v režimu server sloužící jako protistrana pro prvotní testy. Zjištěné hodnoty byly využity pro vhodné nastavení testů, ze kterých se skládají scénáře pokročilého testování. Nesprávné nastavení testů, tedy hlavně velikosti TCP okna a počet TCP toků, vede ke zkreslení naměřených výsledků. Na obrázku 6.6 je mapa haly 1 zobrazující místa (červené body), ve kterých byly provedeny prvotní testy privátní sítě 5G. Dále je zde zobrazena cesta (fialové šipky), během které bylo provedeno testování za pohybu (pomalou chůzí).

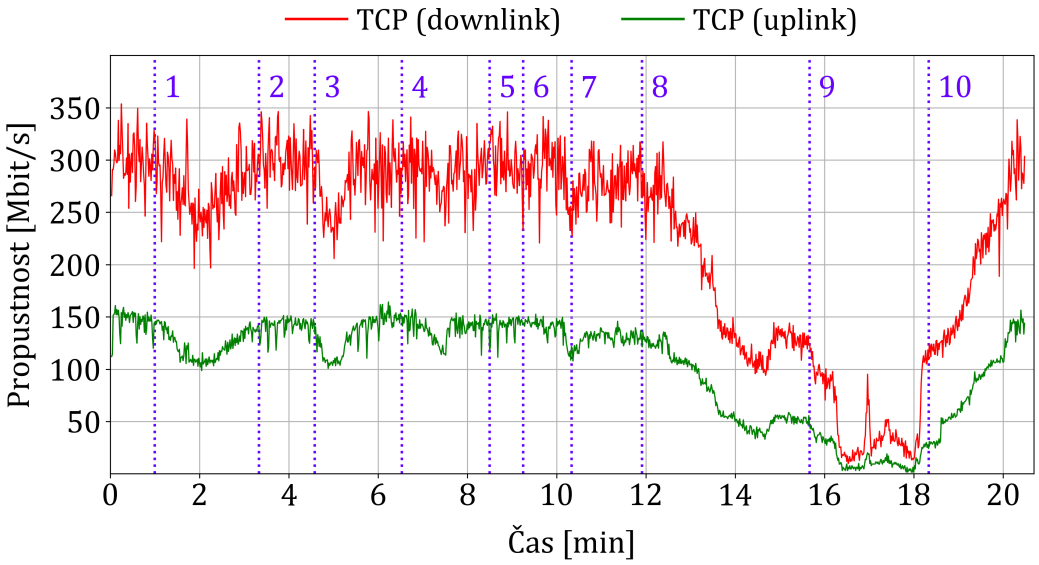


Obrázek 6.6: Mapa haly 1 zobrazující místa a cestu prvotního testování.

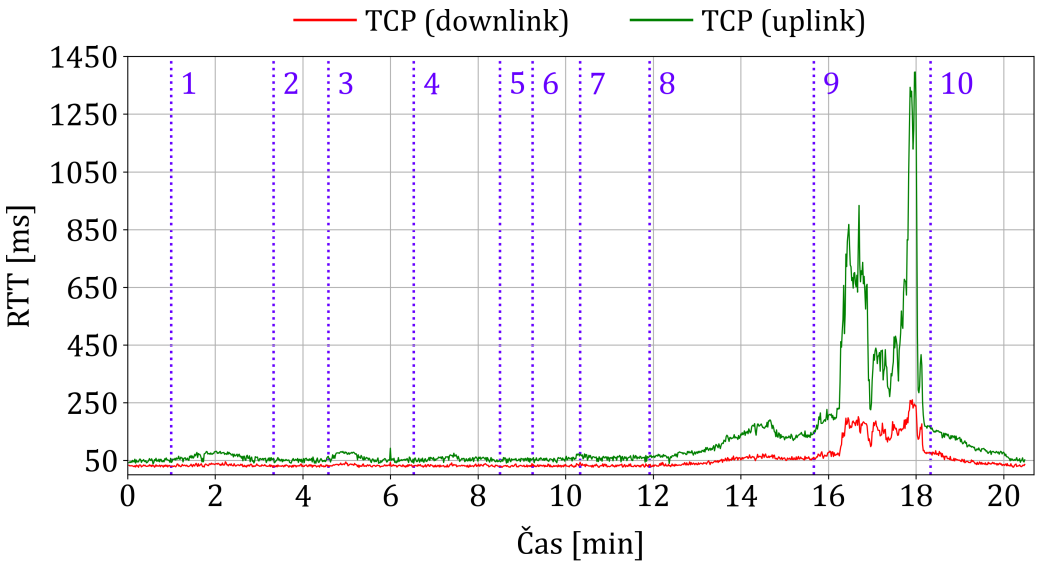
Scénář, který byl využit při testování za pohybu se skládal ze dvou testů typu iPerf3 TCP (pro přenosový směr vzestupný a sestupný) a jednoho testu typu FlowPing. Testy využívající TCP měly nastavenou velikost TCP okna 256 KB, počet TCP toků 6, velikost MSS 1400 B a využívaly algoritmus CUBIC. Aplikace FlowPing (nastavena konstantní přenosová rychlost 100 kbit/s a velikost paketu 128 B) byla spuštěna na pozadí pro validaci ztrátovosti paketů. Naměřenou propustnost sítě zobrazuje obrázek 6.7 a naměřené zpoždění ve smyčce (RTT) obrázek 6.8. Ztrátovost paketů byla 0 % po celou dobu. V těchto obrázcích s grafy jsou v čase vyznačené úseky v halách. Čísla 1 až 6 vyznačují body v hale 1, které jsou také vyznačeny na obrázku 6.6. Úsek mezi čísly 7 a 8 zobrazuje průchod podél stěny v hale 2 sousedící s halou 1. Úsekem mezi čísly 8 a 9 probíhal průchod halou 2 do haly 3. Testování v úseku mezi čísly 9 a 10 probíhalo v hale 3 a v bodě vyznačeném čárou číslo 10 probíhal návrat do haly 1 přes halu 3 a 2. Obrázek 6.9 zobrazuje naměřenou hodnotu RSRP a obrázek 6.10 hodnotu RSRQ. V příloze A.1 jsou parametry signálu zobrazeny v grafech (viz obrázky A.1 a A.2).

Tabulka 6.1 zobrazuje nastavení prvotních testů, ze kterých se skládaly scénáře pro testování. V bodě A byly spuštěny scénáře 1A a 2A. V bodu B byly spuštěny scénáře 1B, 2B, 3B a 4B. Ve scénářích 1A a 3B byl využit test typu iPerf3 TCP

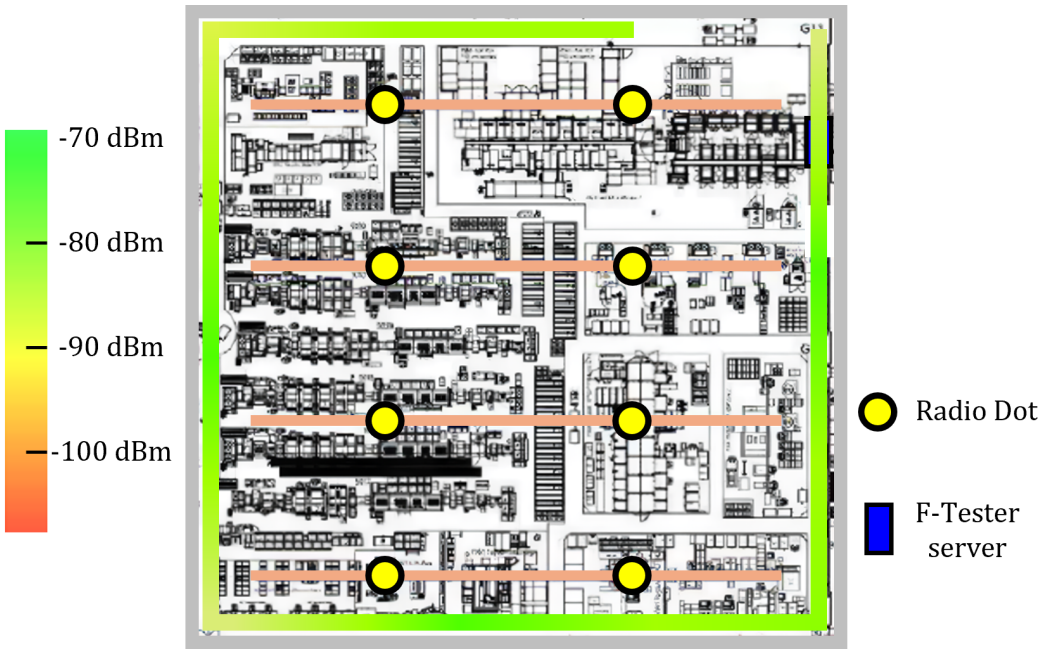
pro oba přenosové směry a test typu FlowPing. Pomocí TCP se nejdříve testoval sestupný směr (downlink) po dobu 60 sekund. Po 30 sekundách od spuštění scénáře se spustily další TCP toky na 60 sekund, které testovaly vzestupný směr (uplink). Velikost MSS byla nastavena na 1400 B. Test typu FlowPing (nastavena konstantní přenosová rychlost 100 kbit/s a velikost paketu 128 B) byl spuštěn na pozadí po celou dobu testování (90 sekund) pro zjištění ztrátovosti paketů. Výslednou propustnost sítě zobrazuje graf na obrázku 6.11 a zpoždění ve smyčce (RTT) zobrazuje graf na obrázku 6.12. Ztrátovost paketů byla 0 % po celou dobu testování. Pro zbylé scénáře jsou grafy propustnosti sítě a zpoždění ve smyčce v příloze A.1. Výsledky prvotních testů v bodech A a B obsahuje tabulka 6.2.



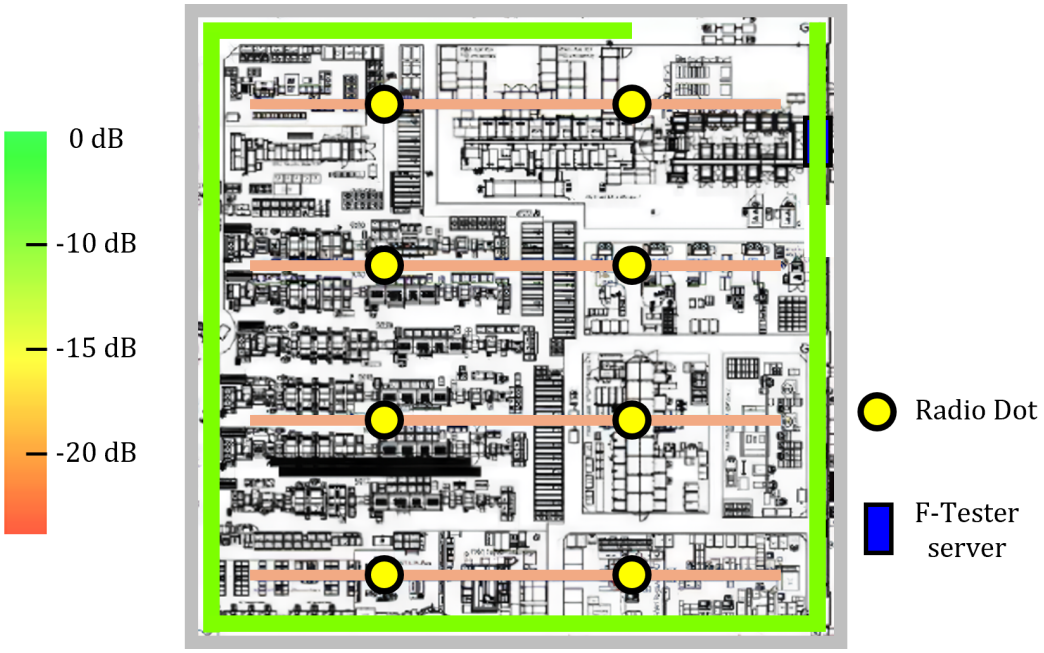
Obrázek 6.7: Graf zobrazující propustnost sítě během testování za pohybu.



Obrázek 6.8: Graf zobrazující RTT během testování za pohybu.



Obrázek 6.9: Mapování naměřené hodnoty RSRP v hale 1.



Obrázek 6.10: Mapování naměřené hodnoty RSRQ v hale 1.

Tabulka 6.1: Nastavení scénářů pro prvotní testování v bodech A a B.

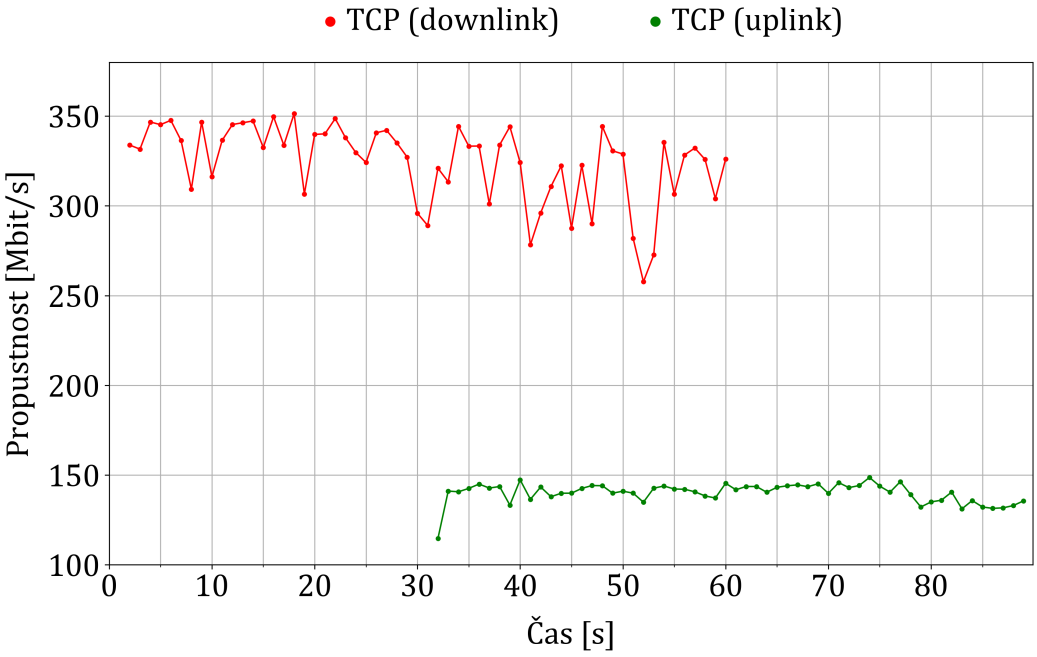
Označení scénáře	Typ testu	Délka trvání [s]	Přenosový směr	Počet toků	Velikost TCP okna [KB]	TCP algoritmus
1A	TCP	60	Downlink	6	256	CUBIC
1A	TCP	60	Uplink	6	256	CUBIC
2A	TCP	100	Downlink	10	512	BBR
1B	TCP	100	Downlink	10	512	BBR
2B	FlowPing	190	Symmetric	-	-	-
3B	TCP	60	Downlink	6	256	CUBIC
3B	TCP	60	Uplink	6	256	CUBIC
4B	TCP	100	Downlink	10	1024	CUBIC

Poznámka: U všech testů byla hodnota MSS nastavena na 1400 B. Na pozadí během testování pomocí scénářů 1A a 3B byla ještě spuštěna aplikace FlowPing (symmetric) s konstantním datovým tokem (přenosová rychlost 100 kbit/s a pakety s velikostí 128 B) pro validaci ztrátovosti paketů.

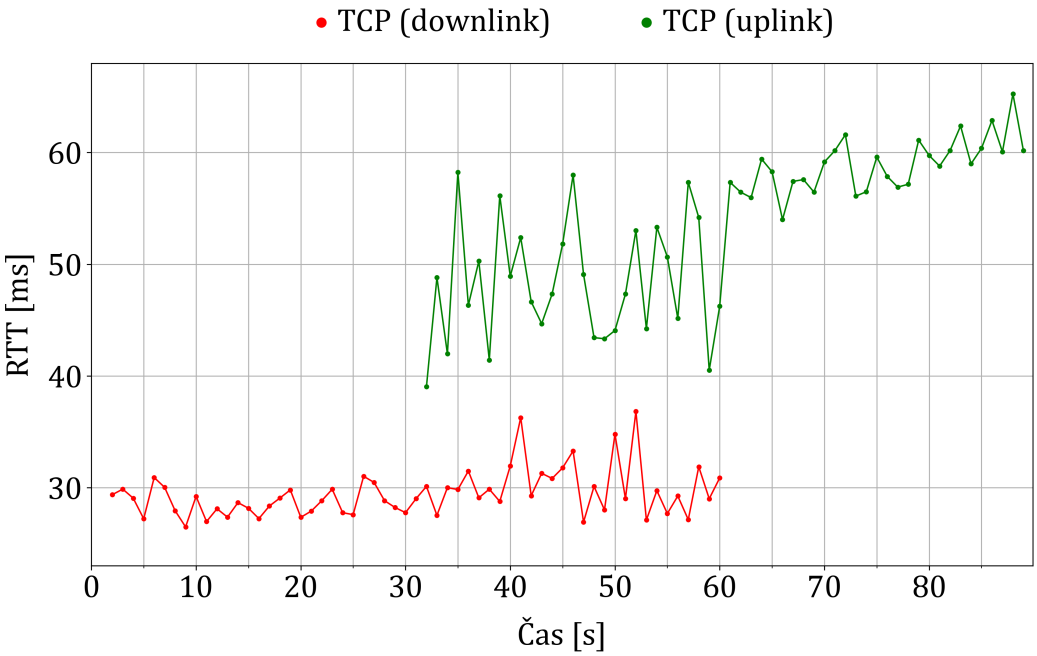
Tabulka 6.2: Výsledky prvotního testování v bodech A a B.

Označení scénáře	Min. propustnost [Mbit/s]	Prům. propustnost [Mbit/s]	Max. propustnost [Mbit/s]	Min. RTT [ms]	Prům. RTT [ms]	Max. RTT [ms]
1A (Downlink)	258	324	351	22	29	40
1A (Uplink)	115	140	149	21	53	73
2A (Downlink)	209	369	419	21	51	67
1B (Downlink)	201	315	385	18	49	78
2B (Symmetric)	10	10	10	17	18	18
3B (Downlink)	151	187	284	25	46	61
3B (Uplink)	59	82	104	58	100	123
4B (Downlink)	193	348	387	46	109	153

Poznámka: U scénářů 1A a 3B byla ztrátovost paketů 0 % po celou dobu testování.



Obrázek 6.11: Graf zobrazující naměřenou propustnost sítě scénářem 1A.



Obrázek 6.12: Graf zobrazující naměřené RTT scénářem 1A.

6.1.3 Vyhodnocení prvotních testů

Základní nastavené hodnoty parametrů privátní sítě 5G pro fyzickou vrstvu byly pro přenosovou rychlost ve vzestupném směru 200 Mbit/s (uplink), v sestupném směru 550 Mbit/s (downlink) a zpoždění v jednom směru přenosu bylo 10 ms. Z testování, při kterém byla maximálně vytěžovaná síť (testy typu iPerf3 TCP například scénářem 1A), vyplynulo, že průměrná propustnost na transportní vrstvě u testů pro vzestupný směr byla okolo 140 Mbit/s a pro sestupný směr byla kolem 320 Mbit/s. Při testování obou přenosových směrů současně docházelo v sestupném směru k poklesu o pár desítek Mbit/s a ve vzestupném směru nikoliv. Avšak ukázalo se, že scénářem 1A nebyla privátní síť 5G maximálně vytížena, tedy nejedná se o naměřenou maximální propustnost. Konstantní hodnota CWND v průběhu testu po většinu času indikuje, že tzv. *úzkým hrdlem* není testovaná síť, což není vyhovující stav pro testování maximální propustnosti sítě. Pokud se hodnota CWND nemění v čase dynamicky, tak limitem může být nastavení testu, přidělená paměť, nedostatečný výkon či nějaký problém u protistrany pro testování, kdy není schopná data přijímat.

K retransmisím paketů docházelo u testů, které měly nastavenou velikost TCP okna 512 KB a 1024 KB. Dále z testování za pohybu vyplynulo, že v rozích haly docházelo k poklesu propustnosti privátní sítě 5G o zhruba 20 %. Přenosová rychlost je nižší na transportní vrstvě ve srovnání s fyzickou vrstvou například kvůli dodatečné režii zaváděné záhlavími paketů, segmentací, detekcí chyb (zabezpečovacím kódem), řízením toku a dalšími mechanismy protokolů. Na rozdíl od domácností je pro průmysl předmětem zájmu přenosová rychlost v obou přenosových směrech dle různých nároků využívaných služeb a u privátních sítí 5G ji lze přenastavit dle potřeb.

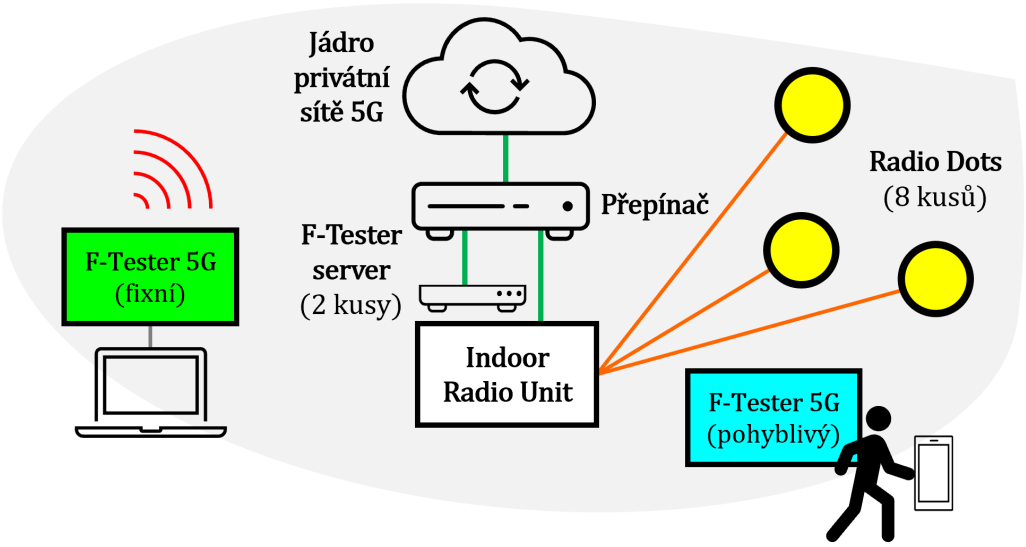
Pro praktické aplikace v průmyslu jsou vypovídající o zpoždění při přenosu testy typu FlowPing. Hodnota RTT (zpoždění ve smyčce) pro jednotlivé pakety, zjištěné aplikací FlowPing (využití UDP), je kolem 18 ms (viz obrázek A.11) a jednosměrné zpoždění je přibližně 9 ms. Hodnota RTT změřená pomocí testu typu iPerf3 TCP odpovídá celému cyklu odeslání bloku dat o velikosti stanoveného TCP okna včetně jeho zpětného potvrzení. Tedy kvůli různým velikostem TCP oken jsou hodnoty RTT jiné oproti naměřenému RTT testem typu FlowPing.

Při vyhodnocování výsledků je důležité brát v potaz nastavení testů (například počet TCP toků, velikost TCP okna a využitý algoritmus proti přetížení) a nastavení testované sítě. Například v bakalářské práci *Testování sítí 5G pro obecné použití a aplikace v průmyslu a energetice* [65] byla testována privátní síť 5G v CIIRC (Český institut informatiky, robotiky a kybernetiky) vybudovaná také společností *T-Mobile* a založená na technologiích od společnosti *Ericsson*. V určitém bodě byla v hale CIIRC dosažena průměrná přenosová rychlost v sestupném směru okolo 500 Mbit/s, pro sestupný směr okolo 65 Mbits/ a zpoždění ve smyčce 18 ms (kmitočtové pásmo 3,5 GHz a šířka pásma 60 MHz). I přesto, že byla využita stejná technologie, kmitočtové pásmo, tak výsledky nelze přímo porovnat, jelikož sítě byly jinak nastavené a při testování byly využity jinak nastavené testy. Také v CIIRC byla menší hala a menší hustota přístupových bodů.

6.2 Vymezení pokročilého testování

V rámci pokročilého testování privátní sítě 5G dne 18. 3. 2024 ve společnosti *Continental Automotive* byly provedeny scénáře ve stacionárních bodech a za pohybu včetně vícebodových zátěžových testů. Na obrázku 6.13 je zobrazeno propojení zařízeních do privátní sítě 5G. Pro testování síťových parametrů privátní sítě 5G byly použity tyto nástroje:

- F-Tester 5G v batohu (pohyblivý),
- F-Tester 5G (fixní),
- dva F-Testery v režimu server jako protistrana pro testy (rozhraní 1GE),
- dvě SIM karty od společnosti *Ericsson*,
- notebook a mobilní telefon.



Obrázek 6.13: Schéma zapojení testování privátní sítě 5G.

Cílem pokročilého testování ve stacionárních bodech a za pohybu bylo:

- ověřit navrženou metodiku popsanou v kapitole 5,
- získat poznatky pro případnou úpravu metodiky,
- testování maximální propustnosti sítě,
- testování konkurence mezi toky v síti (vícebodové zátěžové testy),
- zatěžování sítě dávkovým tokem (burst test),
- zatěžování sítě rostoucím tokem (ramp test),
- testování chování automatického nastavování velikosti TCP okna,
- testování úrovně signálu v hale i mimo halu včetně venkovního prostoru.

6.3 Vícebodové zátěžové testy

Cílem vícebodových zátěžových testů (viz podkapitola 5.3) bylo zkoumání konkurence mezi toky v privátní síti 5G. Obrázek 6.14 zobrazuje F-Tester 5G (fixní) umístěný na dvou F-Testerech (zde byl umístěn po celou dobu testování), které jsou použity jako protistrana pro testy (režim server) pro F-Tester 5G (fixní) a F-Tester 5G (pohyblivý, umístěn v batohu viz obrázek 6.15). Dva F-Testery v režimu server byly využity pro zajištění dostatečné kapacity a výkonu, aby zde nebylo vytvořeno tzv. *úzké hrdlo* a nedocházelo k ovlivňování souběžných testů. Obrázek 6.16 zobrazuje umístění nástrojů pro testování a fialové šipky zobrazují cestu, ve které probíhalo testování za pohybu pomocí F-Testeru 5G (pohyblivý). Přibližně v půlce vyznačeného úseku pro všechny scénáře spuštěné na F-Testeru 5G (pohyblivý) byl test pro daný směr v polovině jeho délky trvání od spuštění. Tedy například ve většině případů v úseku XY byl testován sestupný směr a v úseku YX byl testován vzestupný směr.

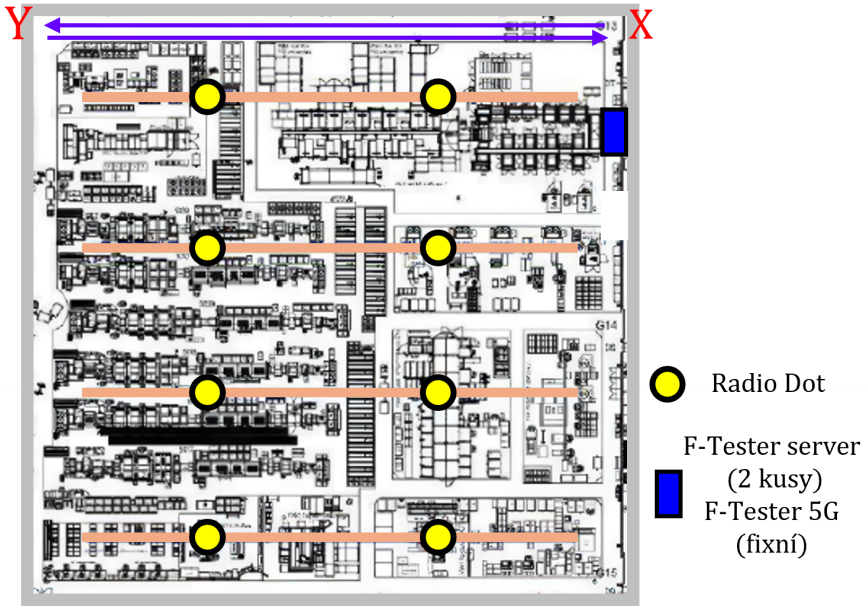
Obrázek 6.17 zobrazuje strukturu scénáře, který byl využit při vícebodových zátěžových testech. V určitý čas byl testován pouze sestupný směr (downlink) a po krátké pauze, pro stabilizaci systému, byt testován sestupný směr (uplink). Tabulka 6.3 obsahuje popis nastavení scénářů, které byly využity pro vícebodové testy. Tabulky 6.4 a 6.5 obsahují výsledky testování pro jednotlivé scénáře. Scénáře byly spouštěny v pořadí, ve kterém jsou v tabulce uvedeny, tedy scénáře A1 a A2 byly spuštěny jako první a scénář R2 byl spuštěn jako poslední v rámci vícebodových testů.

Scénáře jsou označeny písmenem a čísly 1 nebo 2. Číslo 1 označuje scénář, který byl spuštěn na F-Testeru 5G (pohyblivý) a číslo 2 značí scénář, který byl spuštěn na F-Testeru 5G (fixní). Na základě výsledků z prvotních testů (viz podkapitola 6.1.2) vyplynulo, že pro testování pomocí TCP v sestupném směru (downlink) bylo vhodné využívat velikost TCP okna 256 KB, počet TCP toků 10 a algoritmus CUBIC. Pro vzestupný směr (uplink) bylo vhodné využívat velikost TCP okna 256 KB, počet TCP toků 6 a algoritmus CUBIC. Na pozadí byla spuštěna aplikace FlowPing (symmetric) s konstantním datovým tokem (nastavená přenosová rychlost 100 kbit/s a pakety s velikostí 128 B) pro validaci ztrátovosti paketů (PLR).

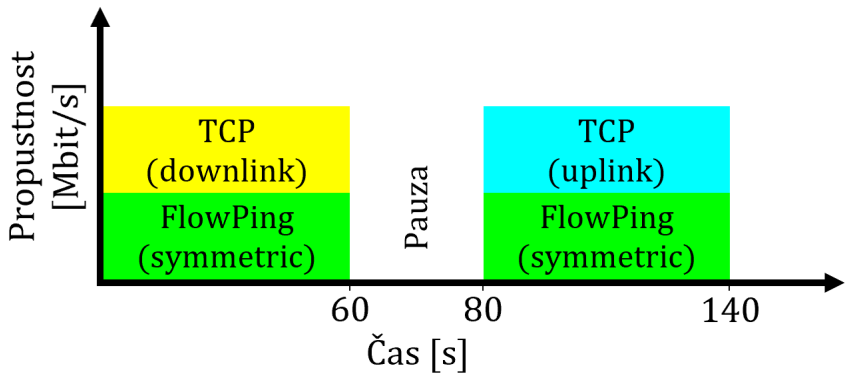
Nastavení TCP testů vycházelo z rovnic 4.1, 4.2 a 4.3. Do těchto rovnic byly dosazeny řádové hodnoty získané pomocí prvotních testů. Pro přenosový směr sestupný (downlink) bylo dosazeno BB = 400 Mbit/s a RTT = 30 ms. Pro směr vzestupný (uplink) bylo dosazeno BB = 150 Mbit/s a RTT = 50 ms. Byla zvolena velikost okna 256 KB, protože během prvotních testů byly detekovány retransmise paketů u testů, které měly nastavenou velikost TCP okna 512 KB a 1024 KB. Dále pokud se síť začne chovat dynamicky (změny síťových parametrů a kvality přenosu), tak při nastavené zbytečně veliké velikosti TCP okna bude dlouho trvat adaptace TCP okna. Například se včas nezjistí, že se zvyšuje ztrátovost paketů, a tím dojde k limitaci propustnosti sítě. Také je nutné brát v úvahu, že při nastavení zbytečně vysoké hodnoty velikosti TCP okna může dojít k přetížení vyrovnávací paměti síťového prvku. Stanovení počtu TCP toků zahrnuje rezervu pro dostatečné vyplnění přenosové kapacity.

Obrázek 6.14: F-Tester 5G (fixní) položen na dvou F-Testerech (režimy server) a IRU jednotce.

Obrázek 6.15: F-Tester 5G v batohu (pohyblivý).



Obrázek 6.16: Mapa haly 1 zobrazující místa a cestu testování za pohybu.



Obrázek 6.17: Struktura scénáře pro vícebodové testy.

Tabulka 6.3: Nastavení scénářů pro vícebodové zátěžové testy.

Označení scénáře	Typ testu	Délka trvání [s]	Přenosový směr	Počet toků	Velikost TCP okna [KB]	TCP algoritmus
A1, A2	TCP	0–60	Downlink	10	256	CUBIC
A1, A2	TCP	80–140	Uplink	6	256	CUBIC
B1, B2	TCP	0–60	Downlink	10	256	CUBIC
B1, B2	TCP	80–140	Uplink	6	256	CUBIC
C1, C2	TCP	0–60	Downlink	10	256	CUBIC
C1, C2	TCP	80–140	Uplink	6	256	CUBIC
C2	UDP	0–30	Downlink	1	-	-
D1, D2, T2	TCP	0–60	Downlink	10	256	CUBIC
D1, D2, T2	TCP	80–140	Uplink	6	256	CUBIC
D2, T2	UDP	0–30	Downlink	1	-	-
Y2, X2	TCP	0–60	Downlink	10	256	CUBIC
Y2, X2	TCP	80–140	Uplink	6	256	CUBIC
Y2, X2	UDP	0–30	Downlink	1	-	-
W2, U2	TCP	0–60	Downlink	10	256	CUBIC
W2, U2	TCP	80–140	Uplink	6	256	CUBIC
E1, E2	TCP	0–60	Downlink	10	256	CUBIC
E1, E2	TCP	80–140	Uplink	6	256	CUBIC
F1	TCP	0–60	Downlink	10	256	CUBIC
F1	TCP	80–140	Uplink	6	256	CUBIC
G1, G2, S2	TCP	0–60	Downlink	10	256	CUBIC
G1, G2, S2	TCP	80–140	Uplink	6	256	CUBIC
R2	TCP	0–60	Downlink	10	256	CUBIC
R2	TCP	80–140	Uplink	6	256	CUBIC
R2	UDP	100–130	Uplink	1	-	-

Poznámka: U testů typu TCP (iPerf3) byla hodnota MSS nastavena na 1400 B a přenosová rychlost pro testy typu UDP (iPerf3) byla nastavena na 100 Mbit/s u scénáře C2, D2, T2, Y2, X2 a 50 Mbit/s u scénáře R2. Velikost paketů pro testy typu UDP byla nastavena na 1200 B. Na pozadí během testování byla spuštěna aplikace FlowPing (symmetric) s konstantním datovým tokem (přenosová rychlost 100 kbit/s a pakety s velikostí 128 B) pro ověření ztrátovosti paketů.

Tabulka 6.4: Naměřená propustnost sítě a RTT pomocí vícebodových zátěžových testů.

Označení scénáře	Min. propustnost [Mbit/s]	Prům. propustnost [Mbit/s]	Max. propustnost [Mbit/s]	Min. RTT [ms]	Prům. RTT [ms]	Max. RTT [ms]
A1 (Uplink)	27,26	65,68	160,70	39,60	147,90	221,70
A1 (Downlink)	334,83	369,20	415,34	27,90	43,90	53,20
A2 (Uplink)	100,83	111,50	132,74	59,70	89,10	108,00
A2 (Downlink)	34,46	43,57	52,47	14,10	37,80	56,10
B1 (Uplink)	25,72	49,37	168,36	38,40	177,20	261,90
B1 (Downlink)	328,88	353,49	407,63	35,80	45,50	53,40
B2 (Uplink)	99,82	115,15	132,73	60,90	85,60	106,90
B2 (Downlink)	33,43	43,87	52,47	14,01	37,90	54,50
C1 (Uplink)	28,29	65,55	155,22	50,50	142,80	210,00
C1 (Downlink)	271,57	340,23	420,46	30,80	47,70	62,50
C2 (Uplink)	98,25	113,68	136,95	58,80	85,30	119,50
C2 (Downlink)	0,00	22,91	49,38	14,07	36,10	99,20
D1 (Uplink)	26,23	51,86	169,73	37,40	169,60	227,50
D1 (Downlink)	275,86	351,32	445,07	30,06	46,50	68,00
D2 (Uplink)	98,01	111,51	135,30	64,60	90,10	109,00
D2 (Downlink)	0,00	23,63	50,92	17,00	36,50	72,10
Y2 (Uplink)	119,85	127,50	132,69	59,70	76,00	108,40
Y2 (Downlink)	0,00	23,91	55,55	16,50	37,10	85,70
X2 (Uplink)	122,87	127,61	137,88	59,60	76,10	91,20
X2 (Downlink)	0,00	23,66	47,84	17,60	37,70	87,60
W2 (Uplink)	113,68	124,92	135,25	62,10	77,40	89,20
W2 (Downlink)	33,95	43,26	51,44	16,80	37,10	53,10
U2 (Uplink)	124,12	129,78	134,59	63,30	75,20	86,70
U2 (Downlink)	270,31	382,13	403,46	32,60	41,90	51,00
T2 (Uplink)	121,15	128,81	136,30	48,50	74,60	130,90
T2 (Downlink)	275,76	336,77	400,80	35,70	48,10	62,10
E1 (Uplink)	26,75	65,71	154,13	42,50	148,60	248,30
E1 (Downlink)	0,00	116,82	415,59	29,06	164,30	503,30
E2 (Uplink)	96,59	112,40	132,13	62,20	88,10	117,60
E2 (Downlink)	343,13	387,40	413,50	30,60	41,30	49,00
F1 (Uplink)	140,64	156,05	176,02	37,70	53,00	68,90
F1 (Downlink)	322,50	406,04	444,98	27,05	38,80	48,30
G1 (Uplink)	26,75	63,58	155,74	40,10	150,30	227,60
G1 (Downlink)	343,57	372,74	428,85	30,04	43,10	69,40
G2 (Uplink)	99,04	115,50	137,11	62,70	86,00	106,90
G2 (Downlink)	32,92	42,51	53,50	16,30	38,10	56,10
S2 (Uplink)	120,74	131,02	137,04	56,70	74,30	88,30
S2 (Downlink)	28,29	44,15	52,98	17,50	38,10	56,20
R2 (Uplink)	75,53	104,52	134,34	61,00	98,20	137,60
R2 (Downlink)	35,49	44,12	51,44	15,50	37,40	55,70

Tabulka 6.5: Naměřená ztrátovost paketů (PLR) během vícebodových zátěžových testů.

Označení scénáře	Přenosový směr	Minimální PLR [%]	Průměrné PLR [%]	Maximální PLR [%]
A1	Uplink	0,00	0,00	0,00
A1	Downlink	0,00	0,00	0,00
A2	Uplink	0,00	0,00	0,00
A2	Downlink	0,00	0,45	3,06
B1	Uplink	0,00	0,00	0,00
B1	Downlink	0,00	0,00	0,00
B2	Uplink	0,00	0,69	3,13
B2	Downlink	0,00	0,05	2,86
C1	Uplink	0,00	0,00	0,00
C1	Downlink	0,00	0,00	0,00
C2	Uplink	0,00	0,00	0,00
C2	Downlink	0,00	10,31	29,90
D1	Uplink	0,00	0,00	0,00
D1	Downlink	0,00	0,00	0,00
D2	Uplink	0,00	0,02	1,02
D2	Downlink	0,00	10,82	36,46
Y2	Uplink	0,00	0,00	0,00
Y2	Downlink	0,00	11,37	33,33
X2	Uplink	0,00	0,00	0,00
X2	Downlink	0,00	11,3	32,02
W2	Uplink	0,00	0,00	0,00
W2	Downlink	0,00	0,39	5,26
U2	Uplink	0,00	0,00	0,00
U2	Downlink	0,00	0,00	0,00
T2	Uplink	0,00	0,00	0,00
T2	Downlink	0,00	0,00	0,00
E1	Uplink	0,00	0,00	0,00
E1	Downlink	0,00	0,00	0,00
E2	Uplink	0,00	0,00	0,00
E2	Downlink	0,00	0,00	0,00
F1	Uplink	0,00	0,00	0,00
F1	Downlink	0,00	0,00	0,00
G1	Uplink	0,00	0,00	0,00
G1	Downlink	0,00	0,00	0,00
G2	Uplink	0,00	0,00	0,00
G2	Downlink	0,00	0,82	5,26
S2	Uplink	0,00	0,00	0,00
S2	Downlink	0,00	0,62	3,09
R2	Uplink	0,00	0,00	0,00
R2	Downlink	0,00	0,49	2,04

6.3.1 Vyhodnocení vícebodových zátěžových testů

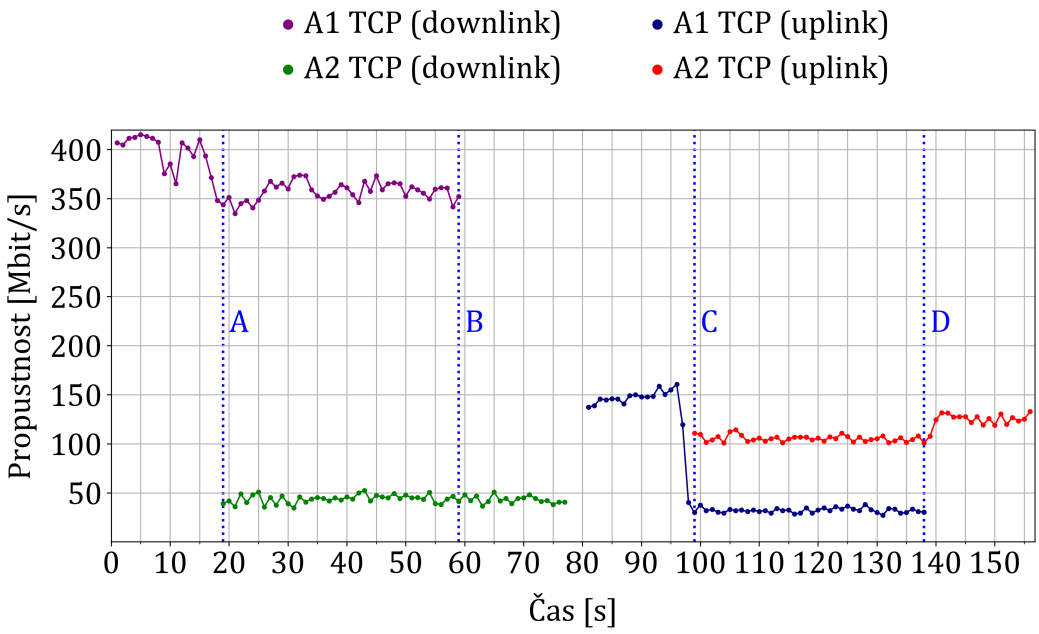
Obrázky 6.18 až 6.21 zobrazují grafy s naměřenými síťovými parametry na transportní vrstvě v čase pro vybrané scénáře. Zbytek grafů je v příloze B.1. Scénáře, které jsou označeny stejným písmenem probíhaly v určitý čas souběžně. Některé scénáře proběhly, když byl jeden F-Tester neaktivní. Sloužily pro zkoumají, jak plánovač základnové stanice přidělí přenosovou kapacitu, která je již k dispozici.

Na obrázku 6.18 pro scénář A1 a A2 je vyznačen úsek AB, ve kterém byl současně testován sestupný směr (downlink) oběma F-Testery. Zde nedošlo k rovnoměrnému přidělení přenosové kapacity. V síti nebyla aplikována žádná prioritizace pro služby nebo vybrané SIM karty (QoS). Pro scénář A1 došlo k poklesu propustnosti o pár desítek Mbit/s. Pro scénář A2 se propustnost pohybovala mezi 34 Mbit/s až 52 Mbit/s, a to i již po uvolnění přenosové kapacity. V rámci zkoumání přidělení přenosové kapacity plánovačem základnové stanice, proběhly některé scénáře, když byl jeden F-Tester neaktivní. Pro scénář Y2 (viz obrázek B.7), během kterého byl F-Tester 5G (pohyblivý) neaktivní, nebyla stále přidělena dostupná přenosová kapacita. Ta byla přidělena, až když F-Tester 5G (fixní) byl po restartu a F-Tester (pohyblivý) byl odpojen z privátní sítě 5G, což proběhlo v rámci scénáře U2 (viz obrázek B.13).

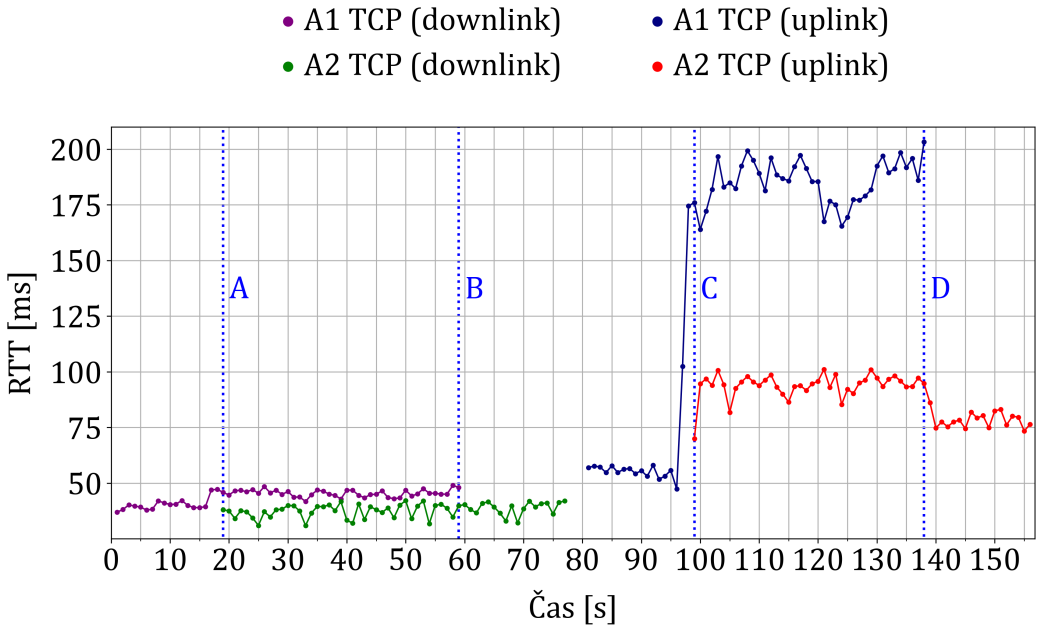
Ve vyznačeném úseku CD (viz obrázek 6.18), kdy byl testován vzestupný směr (uplink), došlo k podobnému jevu, avšak na rozdíl od sestupného směru, zde byla naměřena testem spuštěným na F-Testeru 5G (fixní) vyšší propustnost a po skončení scénáře A1 došlo k mírnému vzrůstu propustnosti. Během spuštěného scénáře A1 nedocházelo k retransmisím paketů v žádném přenosovém směru. Pro scénář A2 ve vzestupném směru také ne, ale v sestupném směru ano. Počet retransmisí paketů byl okolo osmi a testem typu FlowPing byla v průměru naměřena ztrátovost paketů 1 % pro sestupný směr. Dále také nastala situace, kdy pro scénáře s označením E1 došlo k tomu, že F-Testeru 5G (pohyblivý) byla odebrána přenosová kapacita (propustnost dosahovala 0 Mbit/s, viz obrázek B.17) po spuštění TCP toků z F-Testeru 5G (fixní).

Z těchto vícebodových testů vyplynulo doporučení pro navrženou metodiku (viz podkapitola 5.3), že je vhodné mít v síti pro služby nastavené QoS parametry, aby plánovač základnové stanice nepřiděloval přenosovou kapacitu nepředvídatelně. I když nemusí být nastaveny explicitní parametry QoS, tak parametry, jako je úroveň signálu, interference a šum, mohou ovlivnit přidělování přenosové kapacity plánovačem základnové stanice mezi zařízeními. F-Tester 5G (pohyblivý) měl rádiové parametry příznivější pro přenos než F-Tester 5G (fixní).

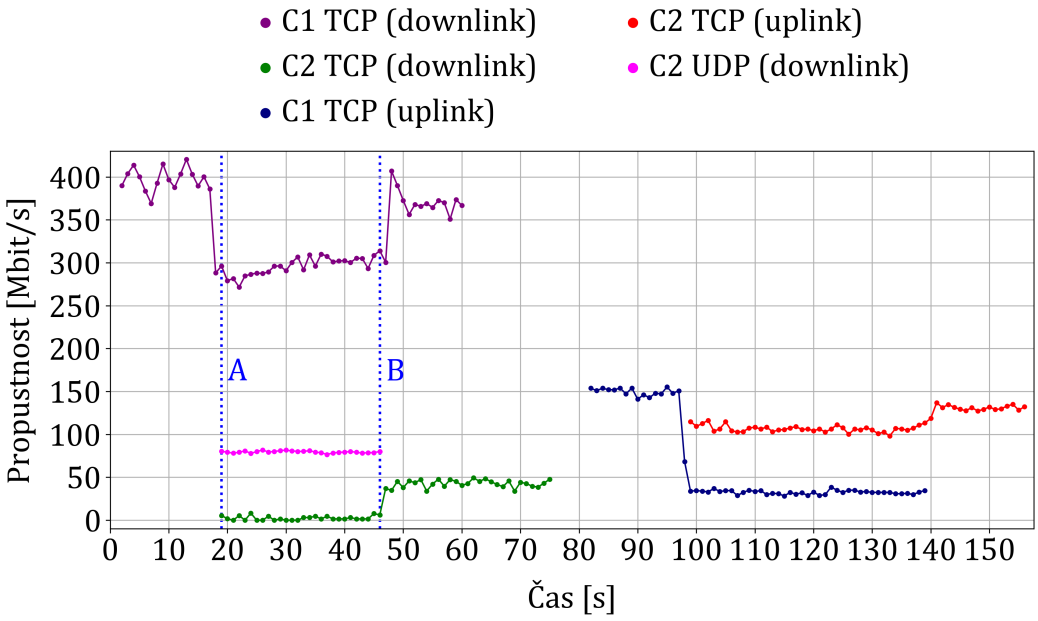
V úseku AB (viz obrázek 6.20) byl v rámci scénáře C2 spuštěn jeden tok UDP s nastavenou přenosovou rychlostí 100 Mbit/s a velikostí paketů 1200 B. To emuluje signály z kamer či stream dat například pro brýle, které budou sloužit pracovníkům pro virtuální realitu. UDP toky jsou dominantní v rámci zabírání kapacity nad TCP toky. To znamená, že TCP toky se přizpůsobují stavu sítě, což se zde projevilo. Během pobíhajícího testu s UDP tokem docházelo u některých TCP toků u scénáře C2 k desítkám retransmisím paketů, bez UDP toku bylo zhruba o polovinu retransmisí méně. Ztrátovost paketů UDP toku se pohybovala mezi 18 % až 24 %. U scénáře C1 nedocházelo k retransmisím paketů.



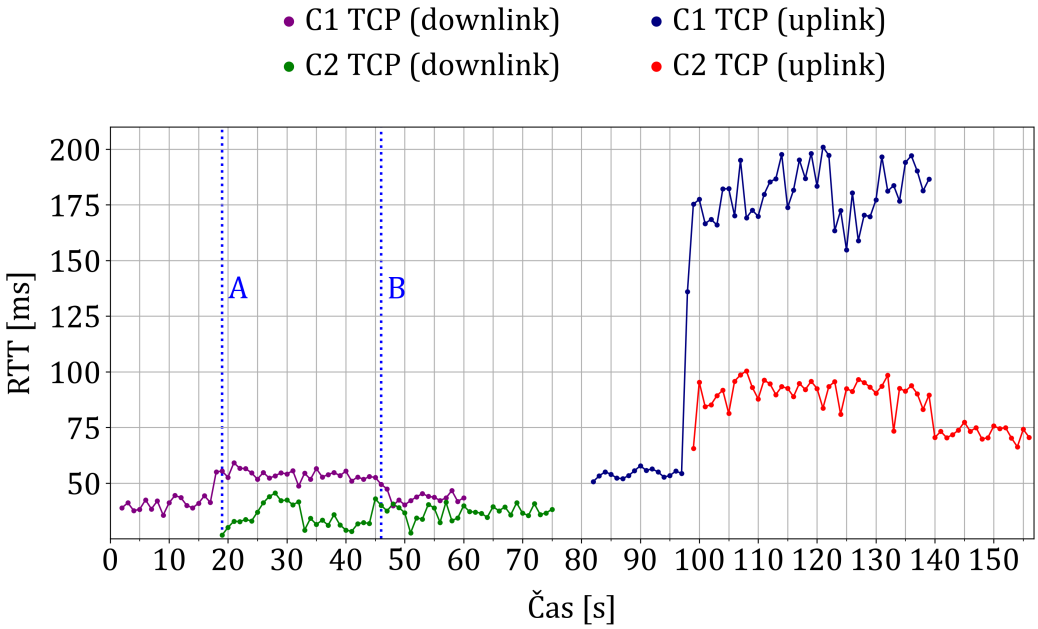
Obrázek 6.18: Graf zobrazující naměřenou propustnost sítě scénářem A1 (pohyb z bodu X do bodu Y a zpět do bodu X) a A2.



Obrázek 6.19: Graf zobrazující naměřené RTT scénářem A1 (pohyb z bodu X do bodu Y a zpět do bodu X) a A2.



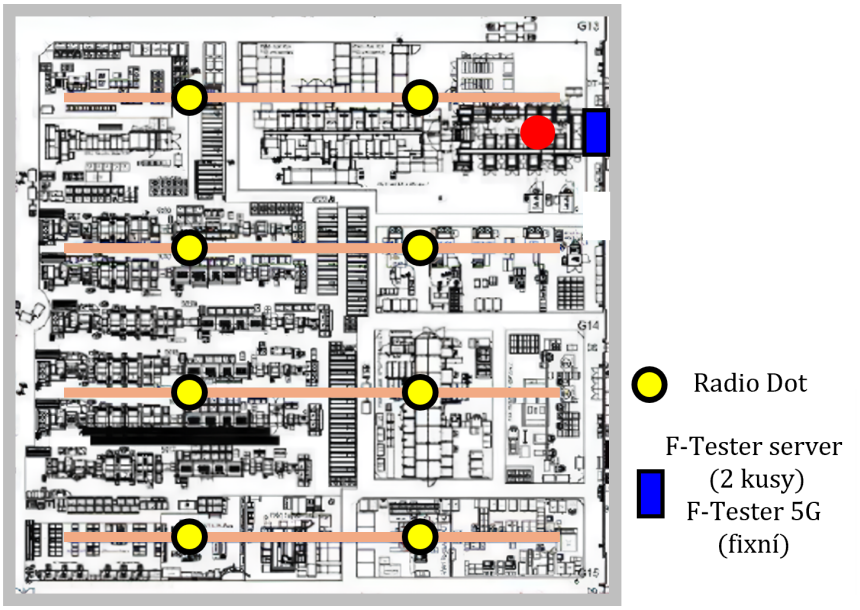
Obrázek 6.20: Graf zobrazující naměřenou propustnost sítě scénářem C1 (pohyb z bodu X do bodu Y a zpět do bodu X) a C2.



Obrázek 6.21: Graf zobrazující naměřené RTT scénářem C1 (pohyb z bodu X do bodu Y a zpět do bodu X) a C2.

6.4 Testování proměnnými toky

Testování proměnnými toky mělo za cíl emulovat určité situace, které mohou v průmyslových sítích nastat. Zatěžování sítě dávkovým tokem (burst test, scénář I1), reprezentuje situaci, kdy dochází k nárazovému vysílání velkého množství dat ze senzorů či dalších zařízeních. Zatěžování sítě rostoucím tokem (ramp test, scénář J1) představuje situaci, při které dochází k postupné aktivaci komunikace různých zařízeních v síti. Obrázek 6.22 zobrazuje červený bod na mapě, kde byly tyto testy provedeny. Tabulka 6.6 obsahuje nastavení jednotlivých scénářů a obrázky 6.23 až 6.26 zobrazují grafy s naměřenými parametry v čase. Při testování scénářem I2 byla ztrátovost paketů 0 % a při testování scénářem J1 začalo docházet ke ztrátovosti paketů (ztrátovost nepřesáhla 0,9 %) od sekundy 168 při propustnosti 148 Mbit/s.

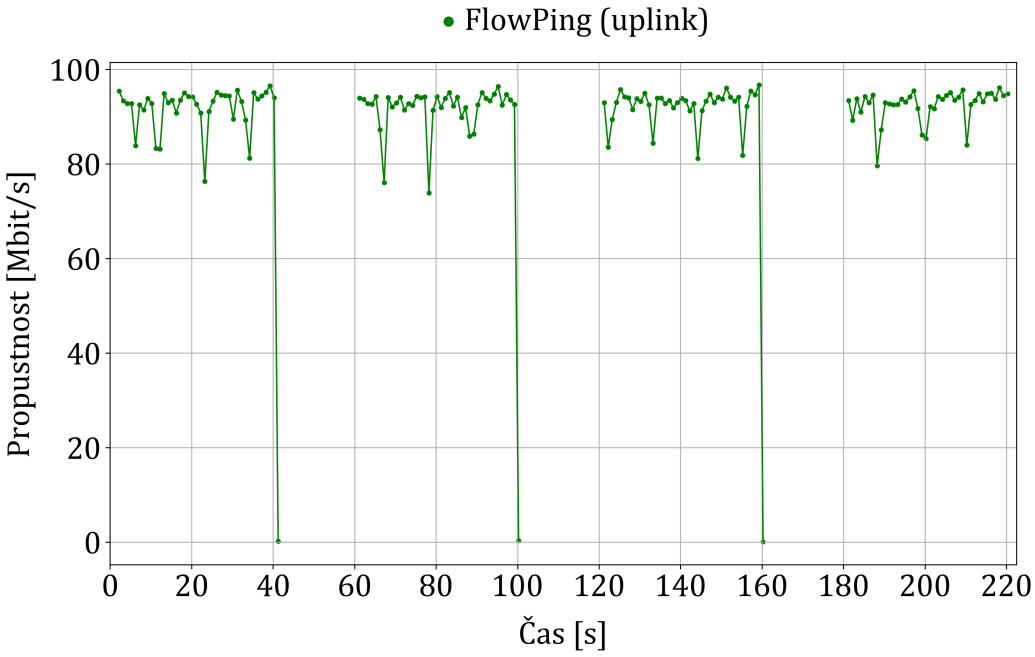


Obrázek 6.22: Mapa haly 1 zobrazující místo testování proměnnými toky.

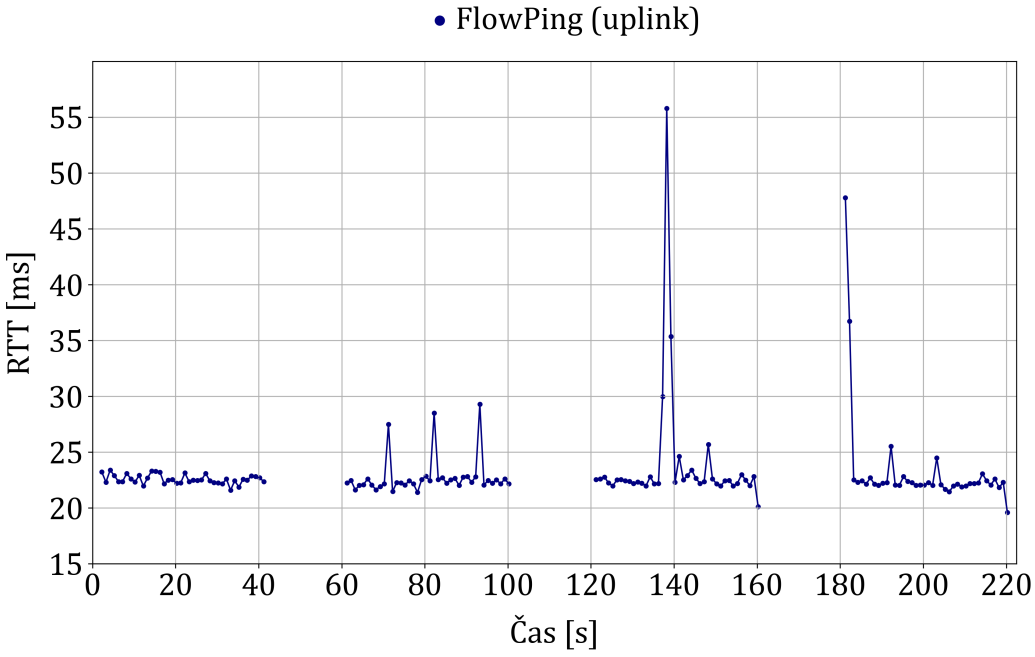
Tabulka 6.6: Nastavení scénářů pro testování proměnnými toky pomocí asymetrického FlowPingu.

Označení scénáře	Typ testu	Časový úsek [s]	Přenosový směr	Přenosová rychlost (start)	Přenosová rychlost (konec)
I1	FlowPing	0–40	Uplink	100 Mbit/s	100 Mbit/s
I1	FlowPing	60–100	Uplink	100 Mbit/s	100 Mbit/s
I1	FlowPing	120–160	Uplink	100 Mbit/s	100 Mbit/s
I1	FlowPing	180–220	Uplink	100 Mbit/s	100 Mbit/s
J1	FlowPing	0–180	Uplink	1 Mbit/s	200 Mbit/s

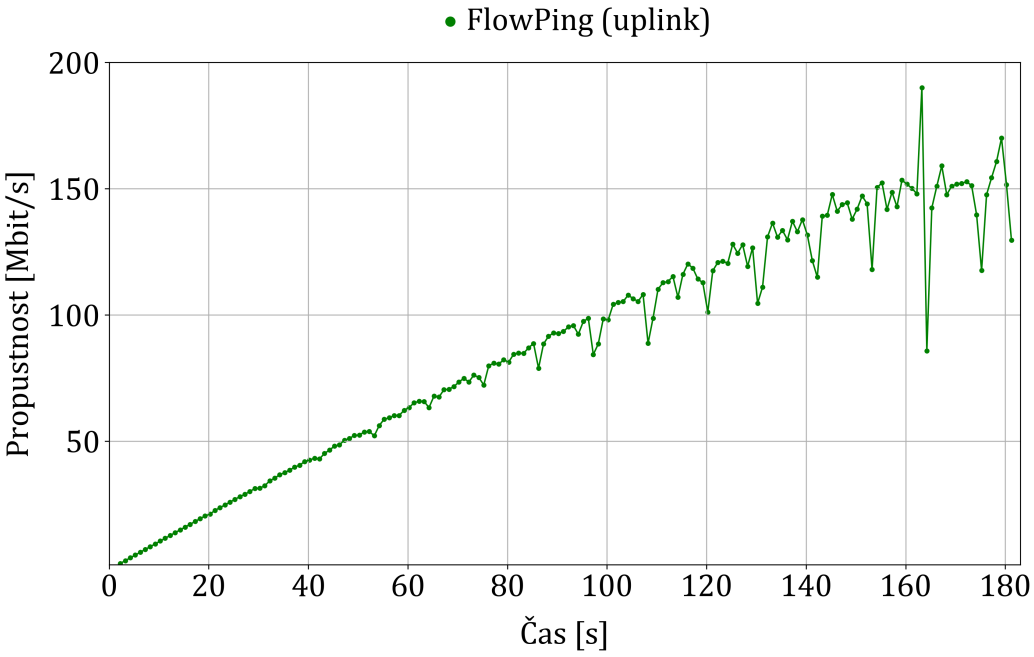
Poznámka: U všech testů byla velikost paketu nastavena na 1400 B.



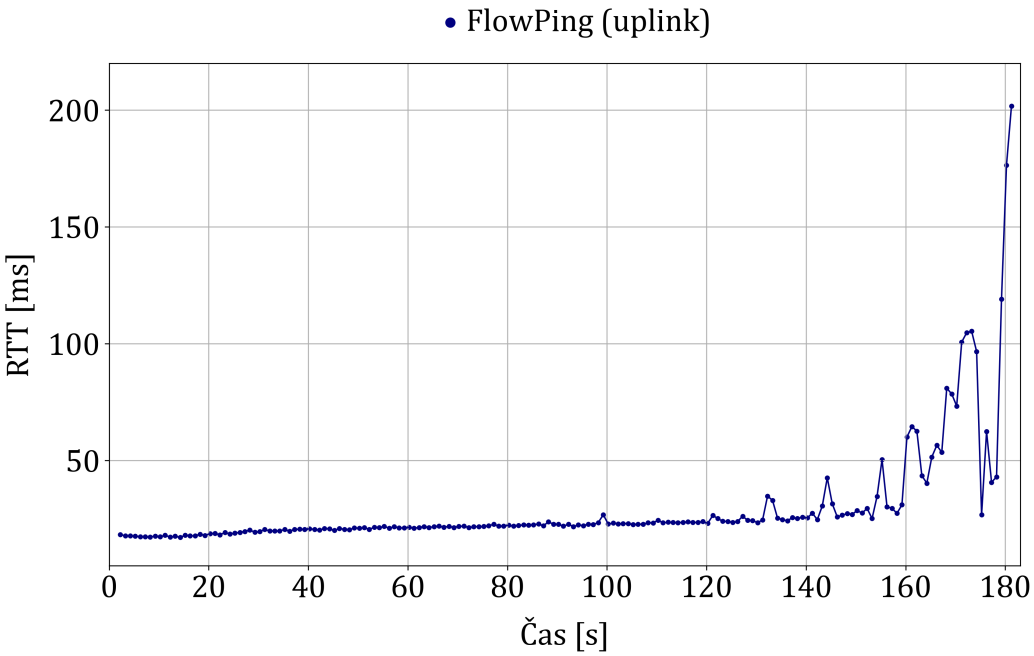
Obrázek 6.23: Graf zobrazující propustnost sítě během spuštěného scénáře I1.



Obrázek 6.24: Graf zobrazující naměřené RTT scénářem I1.



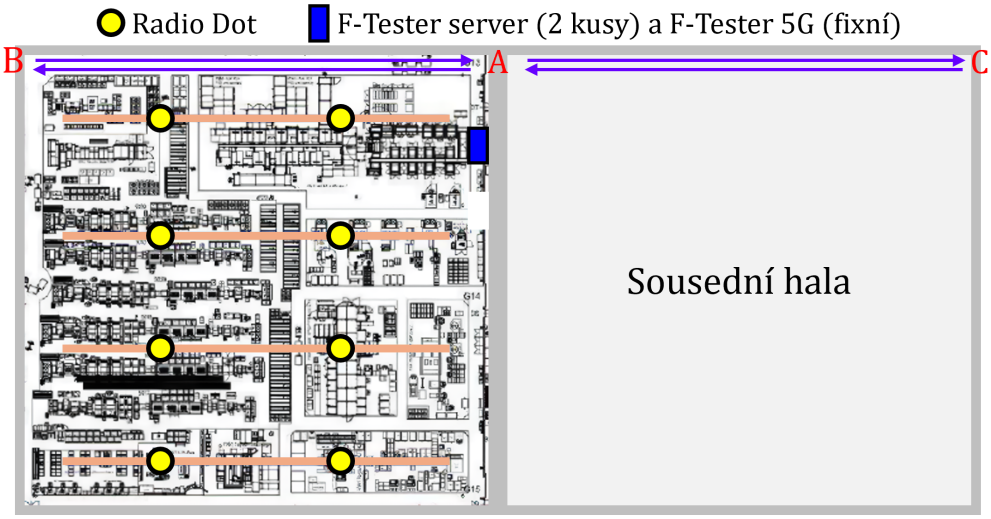
Obrázek 6.25: Graf zobrazující propustnost sítě během spuštěného scénáře J1.



Obrázek 6.26: Graf zobrazující naměřené RTT scénářem J1.

6.5 Testování automatického nastavování velikosti TCP okna

Cílem testování automatického adaptivního nastavování velikosti TCP okna bylo ověřit chování této možnosti pro privátní sítě 5G a následně doporučit jeho využití do navržené metodiky. Zároveň byla testována maximální propustnost sítě. Testování proběhlo pomocí F-Testeru 5G (pohyblivý). Obrázek 6.27 zobrazuje cestu (fialové šipky), ve které probíhaly testy za pohybu (pomalou chůzí). Tabulka 6.7 obsahuje nastavení jednotlivých scénářů. V úseku AB byly spuštěny scénáře N1 a O1. Při přechodu z A do B byl testován sestupný směr (downlink) a vzestupný směr (uplink) při přechodu z B do A. V úseku AC (sousední hala) byly provedeny scénáře P1 a Q1. Sestupný směr (downlink) byl testován při přemístění z A do C a vzestupný směr (uplink) při přemístění z C do A. Přibližně v půlce úseku pro všechny scénáře byl test pro daný směr v polovině jeho délky trvání od spuštění. Výsledky obsahují tabulky 6.8 a 6.9.



Obrázek 6.27: Mapa hal zobrazující cestu měření.

Tabulka 6.7: Nastavení scénářů pro testování automatického TCP okna.

Označení scénáře	Typ testu	Časový úsek [s]	Přenosový směr	Počet toků	Velikost TCP okna [KB]	TCP algoritmus
N1, Q1	TCP	0–60	Downlink	10	0	CUBIC
N1, Q1	TCP	80–140	Uplink	6	0	CUBIC
O1, P1	TCP	0–60	Downlink	10	256	CUBIC
O1, P1	TCP	80–140	Uplink	6	256	CUBIC

Poznámka: U všech testů byla hodnota MSS nastavena na 1400 B. Na pozadí během testování byla spuštěna aplikace FlowPing (symmetric) s konstantním datovým tokem (přenosová rychlost 100 kbit/s a pakety s velikostí 128 B) pro validaci ztrátovosti paketů.

Tabulka 6.8: Naměřená propustnost sítě a RTT.

Označení scénáře	Min. propustnost [Mbit/s]	Prům. propustnost [Mbit/s]	Max. propustnost [Mbit/s]	Min. RTT [ms]	Prům. RTT [ms]	Max. RTT [ms]
N1 (Uplink)	137,35	155,88	172,83	40,90	58,50	82,30
N1 (Downlink)	294,44	420,36	495,85	20,50	76,50	142,20
O1 (Uplink)	140,62	157,88	167,38	37,70	52,10	68,40
O1 (Downlink)	291,84	404,24	440,79	29,80	39,70	99,20
P1 (Uplink)	21,60	64,91	113,67	21,60	64,91	113,67
P1 (Downlink)	160,61	270,58	406,09	30,4	64,40	114,00
Q1 (Uplink)	20,58	44,51	94,72	62,80	132,90	183,20
Q1 (Downlink)	211,23	305,54	397,52	23,9	101,50	152,70

Tabulka 6.9: Naměřená ztrátovost paketů (PLR).

Označení scénáře	Přenosový směr	Minimální PLR [%]	Průměrné PLR [%]	Maximální PLR [%]
N1	Uplink	0,00	0,00	0,00
N1	Downlink	0,00	0,30	13,00
O1	Uplink	0,00	0,00	0,00
O1	Downlink	0,00	0,00	0,00
P1	Uplink	0,00	0,00	0,00
P1	Downlink	0,00	0,00	0,00
Q1	Uplink	0,00	0,00	0,00
Q1	Downlink	0,00	0,00	0,00

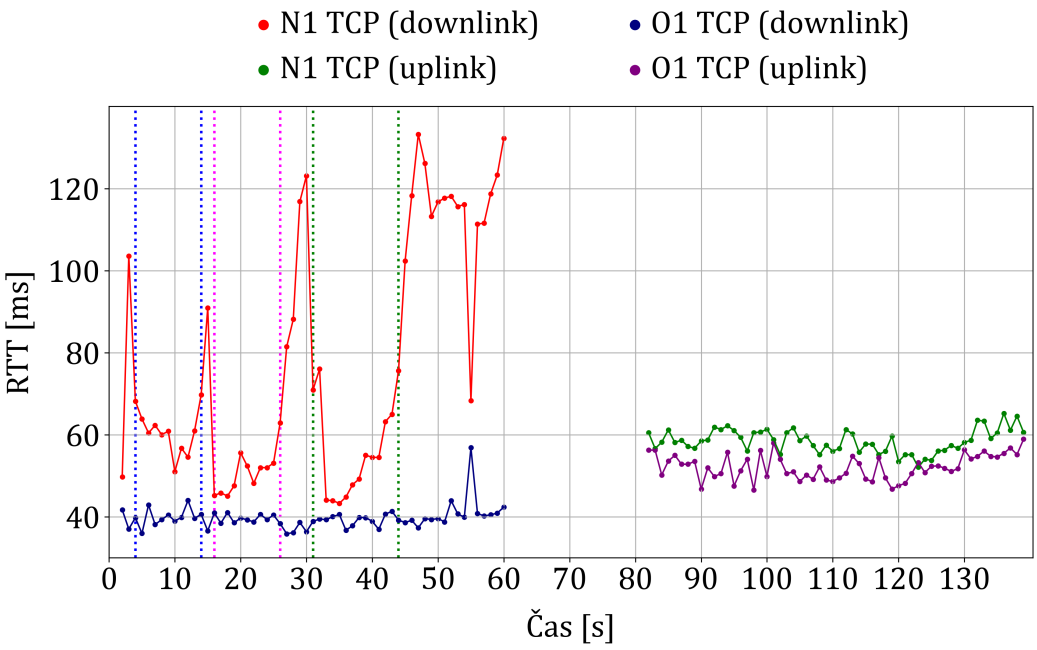
6.5.1 Vyhodnocení testování automatického TCP okna

Obrázek 6.28 zobrazuje graf s naměřeným RTT pro scénáře N1 a O1. Obrázek 6.29 zobrazuje graf s naměřenou propustností sítě pro scénáře N1 a O1 . Zbylé grafy jsou v příloze B.2. Ačkoliv jsou výsledky scénářů vykresleny do společných grafu, tak byly spuštěny v jiný čas. Jsou vykresleny společně, aby byl zobrazen rozdíl chování mezi využíváním pevně nastaveného a automatického TCP okna (množství dat, které jsou do sítě poslána bez potvrzení). Obrázek 6.30 zobrazuje vývoj CWND v čase pro scénář N1 a obrázek 6.31 pro scénář O1.

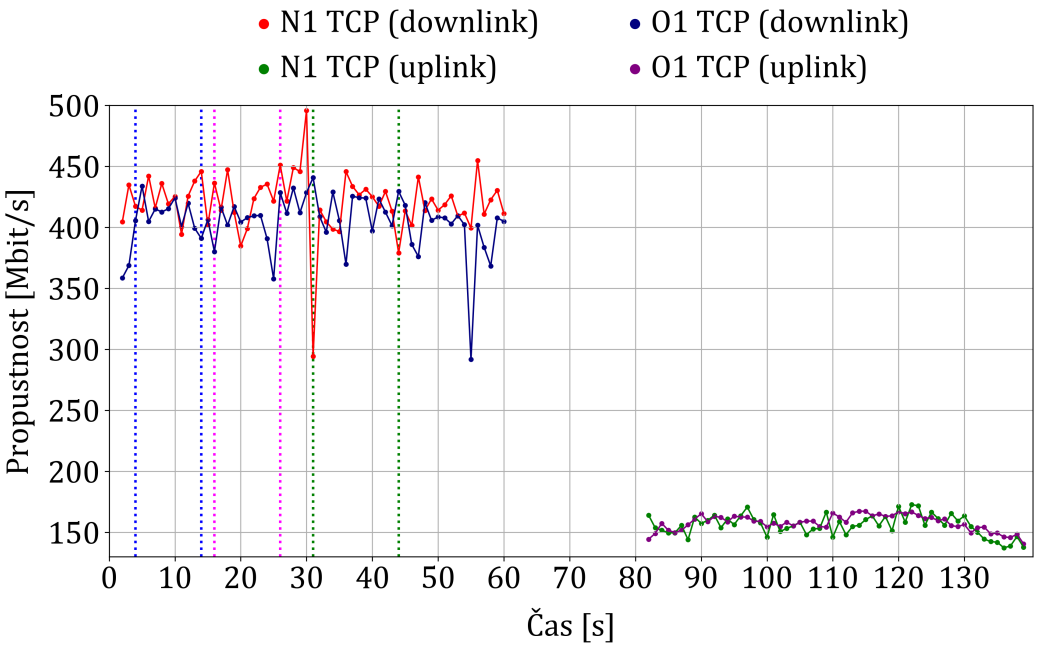
V grafech jsou úseky (vyznačené přerušovanými čarami se stejnou barvou) zobrazující dobu, kdy došlo po výrazném snížení k postupnému navyšování velikosti TCP oken jednotlivých TCP toků pro scénář N1 (viz obrázek 6.30), který měl nastaveno automatické TCP okno. To mělo souvislost s dynamicky se měnící hodnotou RTT (zpoždění ve smyčce), protože se jedná o hodnotu odpovídající celému cyklu odeslání bloku dat o velikosti stanoveného TCP okna včetně jeho zpětného potvrzení. Scénářem N1 byla naměřena v sestupném směru v průměru vyšší propustnost sítě v čase právě kvůli měnící se velikosti TCP okna oproti scénáři O1, který měl nastavenou maximální velikost TCP okna na 256 KB.

Hodnota CWND značí, že pokud se nemění dynamicky (viz obrázek 6.31 pro scénář O1 s nastavenou velikostí TCP okna 256 KB) v čase, tak limitem může být nastavení testu, přidělená paměť, nedostatečný výkon či nějaký problém u protistrany pro testování, kdy není schopná data přijímat. Pokud se hodnota CWND v průběhu testu mění dynamicky, jako tomu je pro scénář N1 s nastaveným automatickým TCP oknem (viz obrázek 6.30), tak to indikuje, že tzv. *úzkým hrdlem* je testovaná síť, což je vyhovující stav pro testování, aby nedošlo ke zkreslení výsledků. Také na tuto dynamickou změnu může mít vliv využívaný TCP algoritmus.

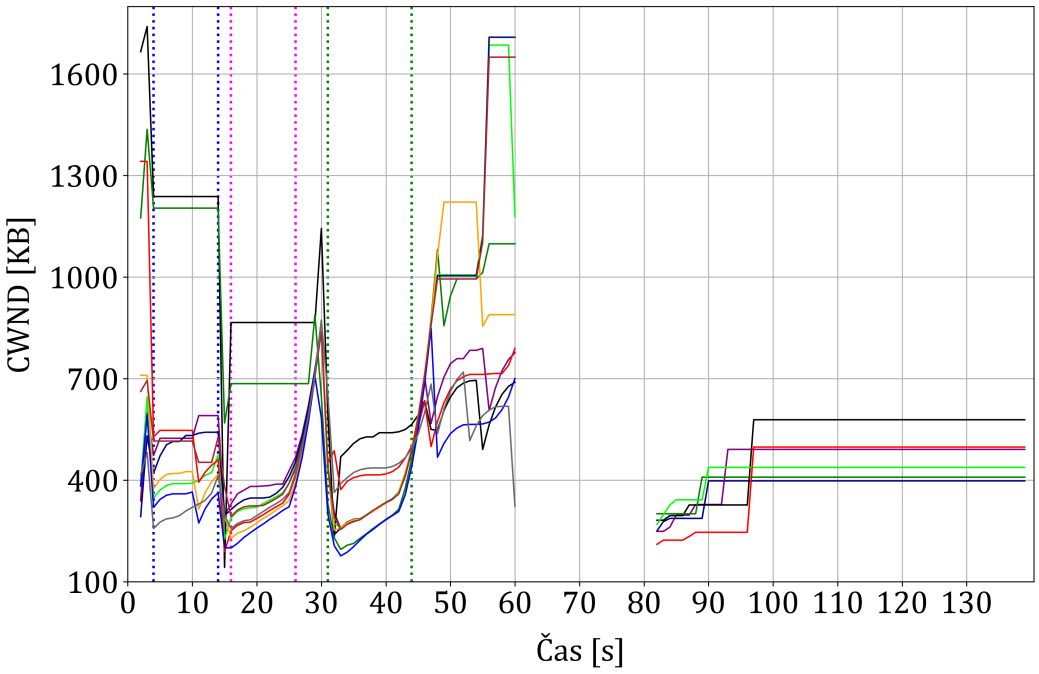
Z testování chování automatického adaptivního nastavování velikosti TCP okna vyplývá, že pro spolehlivé sítě je využívání této možnosti vhodné pro testování maximální propustnosti sítě. Je nutné vzít v potaz to, že pokud nastane ztrátovost paketů při využívání velkého TCP okna, tak dojde k opětovnému poslání celého bloku dat o velikosti stanoveného TCP okna, a tím se snižuje propustnost sítě. To znamená, že při časté ztrátovosti paketů je neefektivní znovu posílat data například o velikosti 1024 KB. Během testování pomocí scénářů O1 a P1 (velikost okna 256 KB) nedocházelo k retransmisím paketů. U scénáře N1 (automatické TCP okno) došlo k retransmisím stovky paketů v čase 15 sekund (ztrátovost paketů 2 %) a 30 sekund (ztrátovost paketů 13 %) během testování sestupného směru (důvod poklesu TCP okna) a ve vzestupném směru nikoliv. Pro scénář Q1 nedocházelo k výraznému počtu retransmisí paketů.



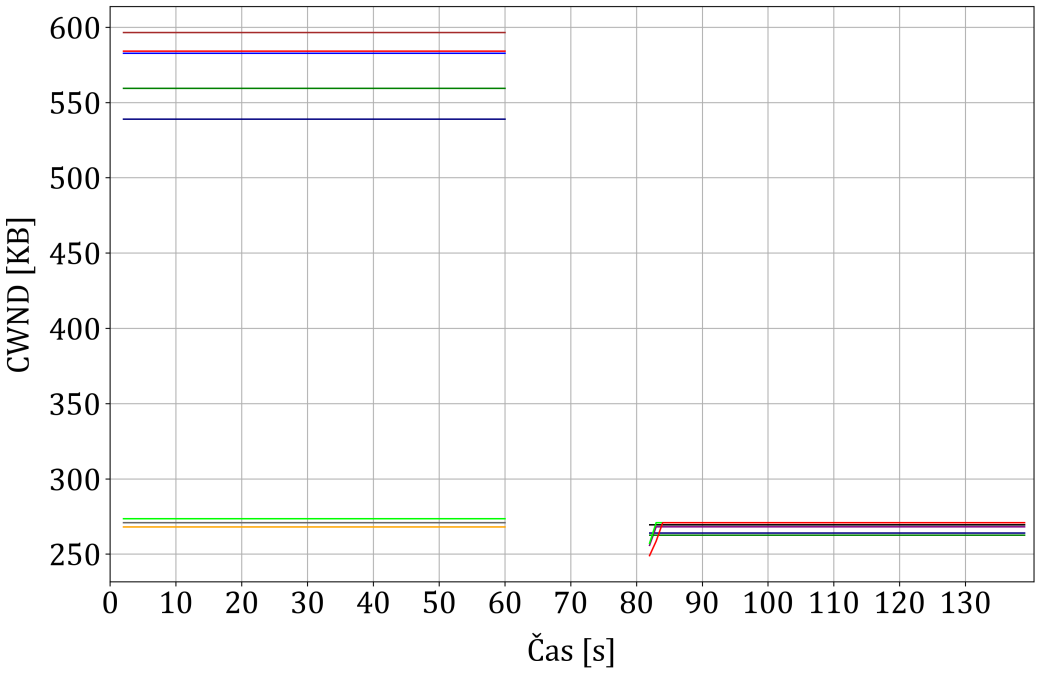
Obrázek 6.28: Graf zobrazující naměřené RTT scénářem N1 (pohyb z bodu A do bodu B a zpět do bodu A) a O1.



Obrázek 6.29: Graf zobrazující propustnost sítě pro scénář N1 (pohyb z bodu A do bodu B a zpět do bodu A) a O1.



Obrázek 6.30: Graf zobrazující rozmezí hodnot CWND během spuštěného scénáře N1 (pohyb z bodu A do bodu B a zpět do bodu A) pro 10 TCP toků (downlink, 0 až 60 s) a 6 TCP toků (uplink, 80 až 140 s).



Obrázek 6.31: Graf zobrazující rozmezí hodnot CWND během spuštěného scénáře O1 (pohyb z bodu A do bodu B a zpět do bodu A) pro 10 TCP toků (downlink, 0 až 60 s) a 6 TCP toků (uplink, 80 až 140 s).

6.6 Vyhodnocení parametrů signálu v hale 1

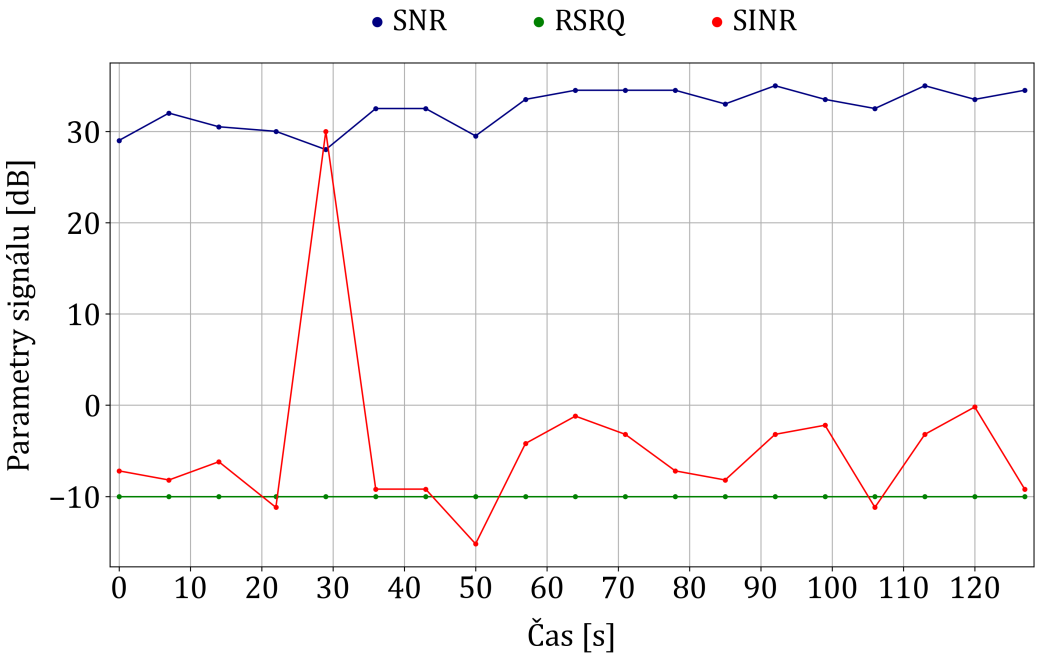
Obrázky 6.32 a 6.33 zobrazují naměřené parametry signálu scénářem O1. Popis těchto parametrů obsahuje podkapitola 2.5. Naměřené hodnoty SNR (průměrně vyšší než 30 dB) a RSRQ (naměřeno -10 dB) se řadí do skupiny velmi dobré. Hodnota SINR (průměrně pod 0 dB) patří do skupiny velmi špatné, protože přístupové body (Radio Dots) v hale 1 byly umístěny blízko u sebe. V síti docházelo k řízené interferenci, ale to je plánovaný stav. To znamená, že SINR parametr není použitelný pro posouzení stavu této sítě. Naměřené hodnoty RSRP a RSSI se řadí do skupiny velmi dobré, jelikož průměrné hodnoty RSRP byly v průměru vyšší než -80 dBm a průměrné hodnoty RSSI byly v průměru vyšší než -65 dBm.

6.7 Testování úrovně signálu mimo halu 1

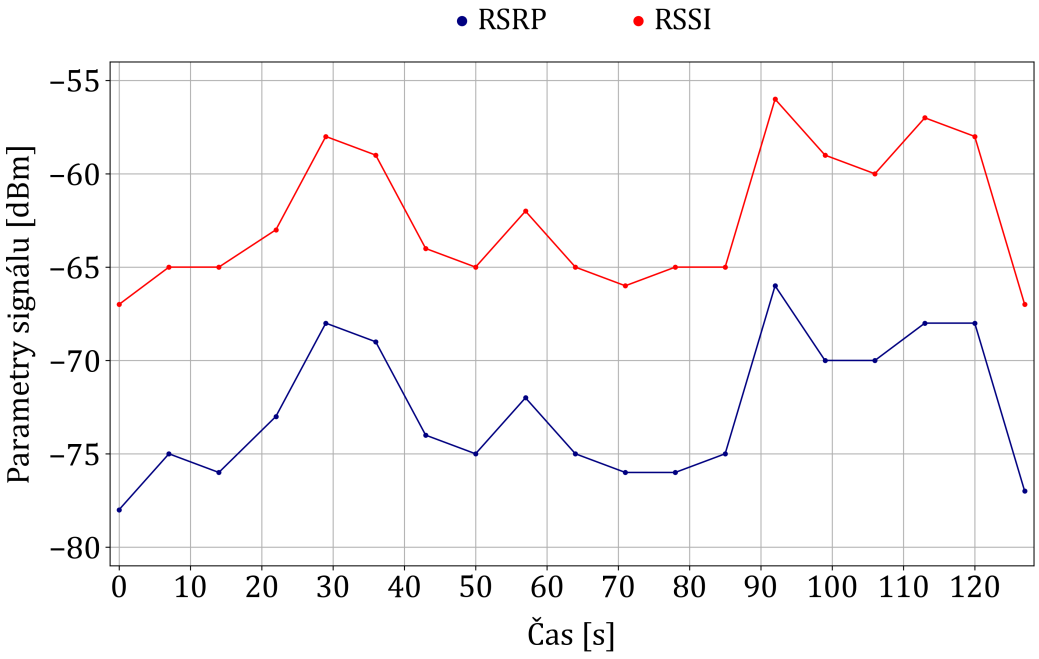
Cílem testování úrovně signálu mimo průmyslový areál bylo zjistit možnost připojení útočníka se SIM kartou do sítě bez nutnosti vstoupit za plot průmyslového areálu. Byl využit test typu iPerf3 TCP (velikost TCP okna 64 KB, 6 TCP toků, MSS 1400 B, algoritmus CUBIC) v sestupném směru (downlink). Testování započalo v místnosti, která sousedí s halou 1. Poté se šlo ven chodbou (dlouhá přibližně 20 metrů), která byla rozdělena dveřmi, až ven z budovy. Tabulka 6.10 obsahuje průběžné hodnoty síťových parametrů. Připojit se k privátní síti 5G za plotem průmyslového areálu nebylo možné, a to ani v blízkosti zdi budovy, ve které jsou výrobní haly. Takže možnost připojení útočníka se SIM kartou k privátní síti 5G mimo budovu nelze, což je vyhovující stav pro bezpečnost.

Tabulka 6.10: Výsledky testování úrovně signálu mimo halu.

Místo	Hodnota RSRQ [dB]	Hodnota RSRP [dBm]	Propustnost v sestupném směru [Mbit/s]
Místnost vedle haly 1	-11	-86	39,77
Začátek chodby vedoucí z budovy	-11	-96	37,78
Prostředek chodby vedoucí z budovy	-12	-111	35,75
Konec chodby vedoucí z budovy	-14	-118	4,10
U vchodu do budovy	-20	-125	0,03



Obrázek 6.32: Graf zobrazující naměřené SNR, RSRQ a SINR scénářem O1 (pohyb z bodu A do bodu B a zpět do bodu A).



Obrázek 6.33: Graf zobrazující naměřené RSRP a RSSI scénářem O1 (pohyb z bodu A do bodu B a zpět do bodu A).

6.8 Doporučení pro rozšiřování pokrytí signálem a diferenciaci služeb

Pokrytí signálem v hale 1 je velmi dobré dle zjištěných parametrů signálu při testování. Pro další haly lze doporučit, že pro pokrytí signálem by bylo možné rozmístit zařízení Radio Dots s menší hustotou (například čtyři). Nicméně pro potřeby geolokace objektů v hale to není vyhovující, protože pro přesnou geolokaci je hustá síť nutná. Problematika pokrytí v průmyslových areálech je popsána v podkapitole 2.5.

Je vhodné využívané služby v privátní síti 5G diferencovat (QoS parametry), tedy přiřadit je do nějaké kategorie, která je vhodně nastavená pro jejich fungování. Jednotlivé typy služeb mají rozdílené potřeby na přenosovou kapacitu a jsou různě citlivé například na zpoždění či ztrátovost paketů. Například nějaká technologie vyžaduje 5 Mbit/s a zpoždění při přenosu nesmí přesáhnout 80 ms, aby byla jistota, že dané úkony v určitém nastavení zvládne.

Diferenciaci služeb v privátní síti 5G je vhodné aplikovat pomocí techniky network slicing, což systém Radio Dots od společnosti *Ericsson* podporuje. Případně lze diferenciaci služeb řešit v rámci Ethernetu (VLAN). V kapitole 3 je popsána problematika diferenciace služeb pro průmysl. Doporučená klasifikace (network slice) jednotlivých služeb, které se zatím řadí mezi očekávané nasazené služby ve společnosti *Continental Automotive*, je:

- **Vysoká priorita** (zpoždění 1 až 10 ms):
  - monitorování stavu výrobních linek (kritické aplikace).
- **Kategorie 1** (přenosová rychlost stovky Mbit/s, zpoždění 1 až 10 ms, ztrátovost paketů 0 %):
  - roboti (výrobní, se senzory či využití strojového vidění),
  - virtuální realita (školení pracovníků či poskytování navádění při práci).
- **Kategorie 2** (přenosová rychlost stovky Mbit/s, zpoždění 1 až 10 ms):
  - autonomní vozidla.
- **Kategorie 3** (přenosová rychlost desítky Mbit/s, zpoždění desítky ms):
  - bezpečnostní kamery,
  - geolokace.
- **Kategorie 4** (přenosová rychlost desítky Mbit/s, zpoždění do sto ms):
  - sběr dat z výrobních strojů pro sledování počtu výrobků a ostatních statistik.
- **Kategorie 5** (přenosová rychlost jednotky Mbit/s, zpoždění stovky ms):
  - zbylý síťový provoz.

Závěr

V rámci této diplomové práce byl nastíněn koncept *Průmysl 4.0*, analyzovány vlastnosti sítí 5G, popsána problematika QoS a diferenciace služeb v komunikačních sítích pro průmysl. Dále práce obsahuje rozbor metod testování pomocí TCP a UDP. Z těchto metod a z dokumentu RFC 6349 se odvíjel návrh metodiky pro testování privátních sítí 5G pomocí platformy F-Tester. Metodika byla ověřena ve společnosti *Continental Automotive* v Brandýse nad Labem, která implementuje privátní síť 5G v rámci výrobního sektoru.

S rostoucími požadavky na digitalizaci průmyslu rostou i nároky na síťovou infrastrukturu, která má zajistit nízké zpoždění při přenosu (zásadní parametr pro automatizaci v průmyslu), vysokorychlostní přenos dat, spolehlivost a vysoký počet připojených zařízení. Těmito vlastnostmi disponuje privátní sít 5G, a tím se stává klíčovou součástí *Průmyslu 4.0*. Vhodné je tyto sítě průběžně monitorovat a testovat. Navržená metodika pro testování privátních sítí 5G pomocí platformy F-Tester je využitelná především pro výkonnostní testování. Popisuje kroky včetně toho, co je nutné vzít v potaz, pro zjištění síťových parametrů a chování sítě pro případy, mezi které se řadí testování maximální propustnosti sítě, testování konkurence mezi TCP a UDP toky v síti pomocí vícebodových zátěžových testů, zatěžování sítě konstantními či proměnnými toky a emulování určitého síťového provozu, kterému může být síť běžně v průmyslu vystavována.

Testování sítí obecně představuje mnoho parametrů volnosti. Jak přesně testovat sítě pomocí TCP není nikde přesně definováno, jelikož existují koncová zařízení využívající například různé algoritmy pro zamezení přetížení sítě jako je CUBIC či BBR. Testování pomocí TCP ovlivňuje mechanismus, pomocí kterého se TCP reguluje. To je důvod, proč každé měřicí zařízení může ukazovat různé výsledky a také je nutné vzít v potaz, jaký je testovací proces, limity hardwaru a jak jsou nastaveny komponenty v síti. Dokument RFC 6349, ze kterého navržená metodika v této práci vychází, neposkytuje návod, jak propustnost sítí testovat, jak postupovat v případě ztrátovosti a jaký algoritmus proti zamezení přetížení vybrat. Důležité je, aby se zapsalo do protokolu nastavení testů TCP a všechny podmínky, za kterých bylo testování vykonáváno. U privátních sítí 5G je výhoda, že je to uzavřený a predikovatelný systém.

Ze scénářů určených pro testování maximální propustnosti (testy typu iPerf3 TCP) privátní sítě 5G ve společnosti *Continental Automotive* vyplynulo, že průměrná propustnost sítě pro vzestupný směr byla okolo 150 Mbit/s a pro sestupný směr byla kolem 400 Mbit/s na transportní vrstvě. Průměrné naměřené zpoždění v jednom směru přenosu se pohybovalo okolo 10 ms. Nastavené hodnoty parametrů privátní sítě 5G pro fyzickou vrstvu v době testování byly pro přenosovou rychlost ve vzestupném směru 200 Mbit/s, v sestupném směru 550 Mbit/s a zpoždění v jednom směru přenosu bylo 10 ms. Přenosová rychlost na transportní vrstvě ve srovnání s fyzickou vrstvou je nižší kvůli dodatečné režii zaváděné záhlavími paketů, detekcí chyb, řízením toku a dalšími mechanismy protokolů.

Během realizace vícebodových zátěžových testů (spuštění testovacích scénářů na více F-Testerech současně) pro zkoumání konkurence mezi TCP a UDP toky v síti nenastalo rovnoměrné přidělování přenosové kapacity, takže plánovač základnové stanice přiděloval přenosovou kapacitu nepředvídatelně. V privátní síti

5G nebyla aplikována žádná prioritizace pro služby nebo vybrané SIM karty (QoS). Z tohoto jevu vyplynulo dodatečné doporučení pro navrženou metodiku, že je vhodné mít v síti pro služby nastavené QoS parametry, aby nebylo přidělování přenosové kapacity nepředvídatelné. V rámci vícebodových testů, kdy byl do scénáře na jednom F-Testeru přidán UDP tok, došlo k očekávanému stavu. Tedy UDP tok byl dominantní v rámci zabírání kapacity nad TCP toky (TCP toky se přizpůsobují stavu sítě). Avšak pro UDP tok, kterému byla nastavená přenosová rychlost na 100 Mbit/s, docházelo ke ztrátovosti paketů okolo 25 %. Při nastavené přenosové rychlosti 50 Mbit/s nikoliv.

Využívání testů s automatickým adaptivním nastavováním velikosti TCP okna pro testování maximální propustnosti privátní sítě 5G v průmyslu je vhodné, jelikož se jedná o spolehlivou síť a o stabilní prostředí. U sítí s dynamicky měnícími se parametry je doporučeno spíše využívat staticky nastavené nižší TCP okno (například 64 či 128 KB) a využívat vyšší počet TCP toků pro nezkreslené testování. Důvodem je to, že pokud dojde například ke ztrátovosti paketů při využívání velkého TCP okna, tak dojde k opětovnému poslání celého bloku dat o velikosti využívaného TCP okna, a tím se snižuje propustnost sítě, a tedy dochází ke zkreslení výsledků testování.

Naměřené hodnoty RSRQ (průměrně naměřeno -10 dB), RSRP (průměrně vyšší než -80 dBm), RSSI (průměrně vyšší než -65 dBm), SNR (průměrně vyšší než 30 dB) se řadí do skupiny velmi dobré a naměřená hodnota SINR (průměrně pod 0 dB) do skupiny velmi špatné. Hodnota SINR byla průměrně pod 0 dB, což bylo příčinou umístění přístupových bodů (Radio Dots) v hale 1, které byly blízko u sebe. V síti dochází k řízené interferenci, ale to je plánovaný stav. To znamená, že SINR parametr není použitelný pro posouzení stavu této sítě.

Bylo také provedeno testování úrovně signálu venku mimo výrobní haly. Z tohoto testování vyplynulo, že připojit se k privátní síti 5G za plotem průmyslového areálu nebylo možné, a to ani v blízkosti zdi budovy, ve které jsou výrobní haly. To je vyhovující stav pro bezpečnost privátní sítě 5G, protože například útočník se SIM kartou se k privátní síti 5G mimo budovu nepřipojí. Obecně umístění přístupových bodů pro pokrytí v průmyslových areálech má dvě hlavní roviny, a to pokrytí určitého prostoru signálem a kapacitní plánování pro služby využívané v průmyslu. Pro další haly společnosti *Continental Automotive* v rámci pokrytí signálem lze doporučit, že by bylo možné rozmístit zařízení Radio Dots s menší hustotou (například čtyři Radio Dots), ale současné rozmístění (osm Radio Dots) je nutné pro službu geolokace objektů, která se zde v budoucnu bude využívat.

V síti je vhodné aplikovat diferenciaci služeb, protože využívané služby pro průmysl mají různé potřeby na přenosovou rychlost, zpoždění či ztrátovost paketů. Tedy rozřadit je do nějaké kategorie (problematika QoS), která je vhodně nastavená pro jejich optimální fungování a dále zajistit, aby kritické služby měly nejvyšší prioritu, aby nenastaly nějaké neblahé následky například na výrobní lince. V privátní síti 5G lze diferenciaci služeb dosáhnou pomocí techniky network slicing, případně to lze řešit v rámci Ethernetu (VLAN). Možné další směřování této práce by mohlo být při vícebodových zátěžových testech využívat vyšší počet F-Testerů 5G nebo provozovat nějaké služby (například brýle pro virtuální realitu) během testování a zároveň mít nastavené nějaké parametry QoS. Další možností je aplikovat navrženou metodiku na privátní síť 5G, která využívá kmitočtové pásmo 26 GHz.

Seznam použité literatury

[1] NÁRODNÍ CENTRUM PRŮMYSLU 4.0. *Analýza českého průmyslu 2024* [online]. 2024. [cit. 2024-03-07]. Dostupné z: https://www.ncp40.cz/files/final-analyza-ceskeho-prumyslu-2024.pdf

[2] CONSTANTINE, Barry, Gilles FORGET, Ruediger GEIB a Reinhard SCHRAGE. *Framework for TCP Throughput Testing* [online]. RFC 6349, 2011. [cit. 2024-02-11]. Dostupné z: https://www.rfc-editor.org/info/rfc6349

[3] NÁRODNÍ CENTRUM PRŮMYSLU 4.0. *Analýza českého průmyslu 2023* [online]. 2023. [cit. 2023-09-25]. Dostupné z: https://www.ncp40.cz/files/analyza-ceskeho-prumyslu-2023-v05.pdf

[4] MAŘÍK, Vladimír. Průmysl 4.0 – aktuální výzvy pro energetiku. In: *Top Expo* [online]. 2017-11-21. [cit. 2023-09-19]. Dostupné z: http://www.top-expo.cz/domain/top-expo/files/smart-city/smart-city-2017/tee/prezentace/marik_vladimir.pdf

[5] MINISTERSTVO PRŮMYSLU A OBCHODU. *Implementace a rozvoj sítí 5G v České republice* [online]. 2021. [cit. 2023-09-19]. Dostupné z: https://www.mpo.cz/assets/cz/e-komunikace-a-posta/elektronicke-komunikace/koncepce-a-strategie/narodni-plan-rozvoje-siti-nga/2020/1/Material-5G_13-12-2019.pdf

[6] PAŠEK, Roman. Průmysl 4.0 – kde se vzal a co to je. In: *SlidePlayer* [online]. 2016-11-30. [cit. 2023-09-19]. Dostupné z: https://slideplayer.cz/slide/1188-8949

[7] BIGELOW, Stephen. Big Data. In: *TechTarget* [online]. 2022. [cit. 2023-09-19]. Dostupné z: https://www.techtarget.com/searchdatamanagement/definition/big-data

[8] *Co je to datová věda?* [online]. Microsoft Azure, 2023. [cit. 2023-09-19]. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-data-science

[9] *Artificial intelligence (AI) vs. machine learning (ML)* [online]. Google Cloud, 2023. [cit. 2023-09-20]. Dostupné z: https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning

[10] SVAZ PRŮMYSLU A DOPRAVY ČESKÉ REPUBLIKY. *Průzkum SP ČR: Firmy se bojí kyberútoků, zlepšují proto ochranu svých dat* [online]. 2023-12-12. [cit. 2023-12-17]. Dostupné z: https://www.spcr.cz/pro-media/tiskove-zpravy/16465-pruzkum-sp-cr-firmy-se-boji-kyberutoku-zlepsuji-proto-ochranu

[11] Záznam Konference Průmysl 4.0 v praxi 2023. In: YouTube [online]. 2023-12-12. [cit. 2023-12-17]. Dostupné z: https://www.youtube.com/watch?v=-zsWywPkMDtM. Kanál uživatele Národní centrum Průmyslu 4.0.

[12] *Understanding important 5G concepts: What are eMBB, URLLC and mMTC?* [online]. Verizon, 2023. [cit. 2023-09-26]. Dostupné z: https://www.verizon.com/about/news/5g-understanding-embb-urllc-mmtc

[13] TOMBAZ, Sibel. Non-standalone and Standalone: two standards-based paths to 5G. In: *Ericsson* [online]. 2022. [cit. 2023-09-26]. Dostupné z: https://www.ericsson.com/en/blog/2023/4/standalone-and-non-standalone-5g-nr-two-5g-tracks

[14] *Využití 5G v businessu* [online]. T-Business, 2023. [cit. 2023-09-26]. Dostupné z: https://t-business.cz/cs/business-reseni/vyuziti-5g-v-businessu

[15] *First Carrier in Japan to Provide 5G Standalone Commercial Services* [online]. SoftBank Corp, 2021. [cit. 2023-09-26]. Dostupné z: https://www.softbank.jp/en/corp/news/press/sbkk/2021/20211019_01

[16] *5G Core* [online]. Ericsson, Inc., 2022. [cit. 2023-09-26]. Dostupné z: https://www.ericsson.com/en/core-network/5g-core

[17] *What is Cloud Native?* [online]. Microsoft, 2023. [cit. 2023-09-27]. Dostupné z: https://learn.microsoft.com/en-us/dotnet/architecture/cloud-native/definition

[18] SIMMONS, Adam. 5G Standalone. In: *Dgtl Infra* [online]. 2023. [cit. 2023-09-27]. Dostupné z: https://dgtlinfra.com/5g-standalone-sa

[19] LAFATA, Pavel a Jiří VODRÁŽKA. *Optické přístupové sítě FTTx a NGA*. 2. přepracované vydání. Praha: České vysoké učení technické v Praze, 2019. ISBN 978-80-01-06552-5.

[20] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Monitorovací zpráva* [online]. 2021. [cit. 2023-10-02]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/ctu/monitorovaci-zprava-c.1/2021/obrazky/mz-2021-1.pdf

[21] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Návrh opatření obecné povahy části plánu využití rádiového spektra č. PV-P/2/XX.2020-YY pro kmitočtové pásmo 24,25–27,5 GHz* [online]. 2021. [cit. 2023-10-02]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/ctu/vyzva-k-uplatneni-pripominek-k-navrhu-opatreni-obecne-povahy-casti-planu-vyuziti-radioveho-spektra-c.pv-p/2/xx.2020-yy-pro-kmitoctove-pasmo-2425-275-ghz/obrazky/pv-rs-2cleanp.pdf

[22] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Připomínky, stanoviska a názory firmy T-Mobile Czech Republic a.s.* [online]. 2021. [cit. 2023-10-02]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/ctu/vyzva-k-uplatneni-pripominek-k-navrhu-opatreni-obecne-povahy-casti-planu-vyuziti-radioveho-spektra-c.pv-p/2/xx.2020-yy-pro-kmitoctove-pasmo-2425-275-ghz/-obrazky/t-mobilep.pdf

[23] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Připomínky, stanoviska a názory firmy Vodafone Czech Republic a.s.* [online]. 2021. [cit. 2023-10-02]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/ctu/vyzva-k-uplatneni-pripominek-k-navrhu-opatreni-obecne-povahy-casti-planu-vyuziti-radioveho-spektra-c.pv-p/2/xx.2020-yy-pro-kmitoctove-pasmo-2425-275-ghz/obrazky/vodafonep.pdf

[24] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Opatření obecné povahy části plánu využití rádiového spektra č. PV-P/2/XX.2020-YY pro kmitočtové pásmo 24,25–27,5 GHz* [online]. 2021. [cit. 2023-10-02]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/ctu/sdeleni-o-vydani-opatreni-obecne-povahy-casti-planu-vyuziti-radioveho-spektra-c.pv-p/2/10.2020-10-pro-kmitoctove-pasmo-2425-275-ghz/obrazky/pvrs-2p.pdf

[25] DELOITTE INSIGHTS. *Technology, Media, and Telecommunications Predictions 2023* [online]. 2022. [cit. 2023-10-02]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/technology-media-telecommunications/TMT-predictions-2023.pdf

[26] *5G technology in industrial campus networks?* [online]. Deutsche Telekom, 2022. [cit. 2023-10-05]. Dostupné z: https://www.telekom.com/en/company/details/5g-technology-in-campus-networks-556692

[27] *5G and Wi-Fi: Charting a path towards superior indoor connectivity* [online]. Ericsson, Inc., 2022. [cit. 2023-10-05]. Dostupné z: https://www.ericsson.com/en/reports-and-papers/5g-and-wi-fi-path-toward-superior-indoor-connectivity

[28] MÜLLER, Zdeněk. Srovnání Wi-Fi a privátních 5G sítí aneb když je licencované pásmo výhodou. In: *Lupa* [online]. 2022. [cit. 2023-10-05]. Dostupné z: https://www.lupa.cz/clanky/srovnani-wi-fi-a-privatnich-5g-siti-aneb-kdyz-je-licencovane-pasmo-vyhodou

[29] BARCLAY, Les. *Propagation of Radiowaves*. 2. vyd. Institution of Engineering and Technology, 2003. ISBN 9780852961025.

[30] *Mobile Signal Strength Recommendations* [online]. Teltonika Networks, 2022. [cit. 2024-03-02]. Dostupné z: https://wiki.teltonika-networks.com/view/Mobile_Signal_Strength_Recommendations

[31] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Metodika pro měření a vyhodnocení datových parametrů mobilních sítí elektronických komunikací.* Verze 2.3 [online]. 2021. [cit. 2023-10-20]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/ctu-new/ochrana-spotrebitele/kontrola-a-mereni/metodika-pro-mereni-a-vyhodnoceni-datovych-parametru-mobilnich-siti-ek-2-3.pdf

[32] ITU-T. *Definitions of terms related to quality of service* [online]. 2008-09-23. [cit. 2024-02-03]. Dostupné z: https://www.itu.int/rec/T-REC-E.800-200809-I/en

[33] ETSI. *Technical Report 102 157* [online]. 2003. [cit. 2024-02-03]. Dostupné z: https://www.etsi.org/deliver/etsi_tr/102100_102199/102157/01.01.01_60/tr_102157v010101p.pdf

[34] ITU-T. *General aspects of quality of service and network performance in digital networks, including ISDNs* [online]. 1993-03-01. [cit. 2024-02-03]. Dostupné z: https://www.itu.int/rec/T-REC-I.350-199303-I/en

[35] ITU-T. *Framework and methodologies for the determination and application of QoS parameters* [online]. 2007-02-08. [cit. 2024-02-03]. Dostupné z: https://www.itu.int/rec/T-REC-E.802-200702-I/en

[36] ITU-T. *Quality of Service regulation manual* [online]. 2017. [cit. 2024-02-03]. Dostupné z: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.QOS_REG01-2017-PDF-E.pdf

[37] ITU-T. *Vocabulary for performance, quality of service and quality of experience* [online]. 2017-11-13. [cit. 2024-02-03]. Dostupné z: https://www.itu.int/rec/T-REC-P.10-201711-I/en

[38] BEZPALEC, Pavel. *Analýza zpoždění v IP telefonním systému I.* [online]. 2008-05-09. [cit. 2024-02-04]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2008050004

[39] BEZPALEC, Pavel. *Analýza zpoždění v IP telefonním systému II.* [online]. 2008-05-09. [cit. 2024-02-04]. Dostupné z: http://access.feld.cvut.cz/view.php?nazevclanku=analyza-zpozdeni-v-ip-telefonnim-systemu-ii&cisloclanku=2008050003

[40] *Understanding Delay in Packet Voice Networks* [online]. Cisco Systems, Inc., 2006-02-02. [cit. 2024-02-04]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/5125-delay-details.html

[41] *Header Compression* [online]. Cisco Systems, Inc., 2006-01-30. [cit. 2024-02-05]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/header_compression.html

[42] *Reducing Latency and Jitter for Real-Time Traffic Using Multilink PPP* [online]. Cisco Systems, Inc., 2016-02-14. [cit. 2024-02-05]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_latjit/configuration/xe-16/qos-latjit-xe-16-book/qos-red.html#GUID-DCB20ADF-1F8E-434B-AE97-54802879F34F

[43] CISCO. *Cisco IOS Quality of Service Solutions Configuration Guide* [online]. Cisco Systems, Inc., 2009-11-20. [cit. 2024-02-05]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book.pdf

[44] CISCO. *Compare Traffic Policy and Traffic Shape to Limit Bandwidth* [online]. Cisco Systems, Inc., 2023-09-07. [cit. 2024-02-05]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

[45] CISCO. *Configuring VLANs* [online]. Cisco Systems, Inc. [cit. 2024-03-03]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html#con_1273307

[46] KALØR, Anders, René GUILLAUME, Jimmy NIELSEN, Andreas MUELLER a Petar POPOVSKI. *Network Slicing in Industry 4.0 Applications: Abstraction Methods and End-to-End Analysis* [online]. 2018, vol. 14, no. 12, s. 5419-5427. [cit. 2024-03-03]. DOI: 10.1109/TII.2018.2839721. Dostupné z: https://vbn.aau.dk/ws/portalfiles/portal/306349947/Network_Slicing_in_Industry_4.0_Applications_Abstraction_Methods_and_End_to_End_Analysis.pdf

[47] ITU-T. *Guidelines for the definition of SLA representation templates* [online]. 2006-07-14. [cit. 2024-02-06]. Dostupné z: https://www.itu.int/rec/T-REC-M.3342-200607-I

[48] VODRÁŽKA, Jiří a Petr JAREŠ. *Testování nové generace internetových přípojek (NGA)* [online]. Portál inovace vyššího odborného vzdělávání, 2019. [cit. 2023-10-20]. Dostupné z: https://www.vovcr.cz/odz/tech/521/page00.html

[49] *FlowPing – UDP based ping application* [online]. [cit. 2023-10-20]. Dostupné z: https://flowping.fel.cvut.cz

[50] Originální nástroj FlowPing a jeho využití v F-Testeru pro měření 5G sítí. In: YouTube [online]. 2023-04-11. [cit. 2023-10-20]. Dostupné z: https://www.youtube.com/watch?v=TzvzMqGbaQk. Kanál uživatele PROFiber Networking.

[51] E-Shaper. Produktový list. In: *F-Tester NGA – 5G* [online]. [cit. 2023-10-20]. Dostupné z: https://f-tester.fel.cvut.cz/portal/wp-content/uploads/2022/01/EShaper_v1.pdf

[52] *iPerf – The ultimate speed test tool for TCP, UDP and SCTP* [online]. [cit. 2023-10-20]. Dostupné z: https://iperf.fr

[53] iPerf3 aneb Měřit pouze maximální propustnost je nesmysl, pojďme to dělat lépe. In: YouTube [online]. 2024-02-07. [cit. 2024-02-11]. Dostupné z: https://www.youtube.com/watch?v=5Z_GMM2KBz0. Kanál uživatele CSNOG.

[54] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Metodika pro měření a vyhodnocení datových parametrů pevných sítí elektronických komunikací.* Verze 2.1 [online]. 2021. [cit. 2023-10-20]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/ctu-new/ochrana-spotrebitele/kontrola-a-mereni/metodika-pro-mereni-a-vyhodnoceni-datovych-parametru-pevnych-siti-ek-2-1.pdf

[55] HUSTON, Geoff. BBR, the new kid on the TCP block. In: *APNIC* [online]. 2017-05-09. [cit. 2023-12-11]. Dostupné z: https://blog.apnic.net/2017/05/09/bbr-new-kid-tcp-block

[56] CARDWELL, Neal et al. BBR: Congestion-Based Congestion Control. In: *Communications of the ACM* [online]. 2017. [cit. 2023-12-11]. Dostupné z: https://cacm.acm.org/magazines/2017/2/212428-bbr-congestion-based-congestion-control

[57] CARDWELL, Neal et al. BBR Congestion Control: IETF 99 Update. In: *The Internet Engineering Task Force* [online]. 2017-07-17. [cit. 2023-12-11]. Dostupné z: https://www.ietf.org/proceedings/99/slides/slides-99-iccrg-iccrg-presentation-2-00.pdf

[58] *F-Tester – měření datových sítí* [online]. [cit. 2023-12-14]. Dostupné z: https://f-tester.fel.cvut.cz

[59] Multifunkční testery – ČVUT F-Tester NGA. In: *PROFiber Networking CZ s.r.o.* [online]. [cit. 2023-12-14]. Dostupné z: https://www.profiber.eu/cz/merici-technika-transport-a-datakom/multifunkcni-testery/Cvut-f-tester-nga/#productdetail

[60] Multifunkční testery – ČVUT F-Tester 5G. In: *PROFiber Networking CZ s.r.o.* [online]. [cit. 2023-12-14]. Dostupné z: https://www.profiber.eu/cz/merici-technika-transport-a-datakom/multifunkcni-testery/-Cvut-f-tester-5g

[61] *Zrychlili jsme provoz i komunikaci v Continental* [online]. T-Business, 2023. [cit. 2023-12-13]. Dostupné z: https://t-business.cz/cs/aktuality/aktualita/continental

[62] *Radio Dots* [online]. Ericsson, Inc. [cit. 2023-12-13]. Dostupné z: https://www.ericsson.com/en/portfolio/networks/ericsson-radio-system/radio/small-cells/indoor/radio-dots

[63] *Indoor Radio Unit* [online]. Ericsson, Inc. [cit. 2023-12-13]. Dostupné z: https://www.ericsson.com/en/portfolio/networks/ericsson-radio-system/radio/small-cells/indoor/indoor-radio-unit

[64] Virtuální realita je v brandýském závodě Continental Automotive běžným nástrojem. In: *Lupa* [online]. 2023-08-22. [cit. 2023-12-13]. Dostupné z: https://www.lupa.cz/pr-clanky/virtualni-realita-je-v-brandyskem-zavodu-continental-beznym-nastrojem

[65] POBOŘIL, Vít. *Testování sítí 5G pro obecné použití a aplikace v průmyslu a energetice*. Praha, 2022. Bakalářská práce. ČVUT v Praze, Fakulta elektrotechnická, Katedra telekomunikační techniky.

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

3GPP 3rd Generation Partnership Project

4G Mobilní sítě čtvrté generace

5G Mobilní sítě páté generace

AI Artificial Intelligence

APU Accelerated Processing Unit

BB Bottleneck Bandwidth

BBR Bottleneck Bandwidth and Round-trip

BDP Bandwidth Delay Product

BER Bit Error Ratio

BERT Bit Error Rate Test

CBR Constant Bit Rate

CBWFQ Class-Based Weighted Fair Queuing

CIIRC Český institut informatiky, robotiky a kybernetiky

CQ Custom Queuing

CRC Cyclic Redundancy Check

CSV Comma Separated Values

CWND Congestion Window

ČTÚ Český telekomunikační úřad

DSCP Differentiated Services Code Point

eMBB enhance Mobile Broadband

ES Errored Seconds

ETSI European Telecommunications Standards Institute

FDD Frequency Division Duplex

FIFO First In First Out

FTP File Transfer Protocol

GE Gigabit Ethernet

gNB Next Generation Node B

HTTPS Hypertext Transfer Protocol Secure

ID Identifier

IEEE Institute of Electrical and Electronics Engineers

IMEI International Mobile Equipment Identity

IoT Internet of Things

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IRU Indoor Radio Unit

ISO International Organization for Standardization

IT Information Technology

ITU International Telecommunication Union

ITU-T ITU Telecommunication Standardization Sector

JSON JavaScript Object Notation

LLQ Low-Latency Queuing

MIMO Multiple Input Multiple Output

ML Machine Learning

mMTC Massive Machine Type Communication

MSS Maximum Segment Size

MTU Maximum Transmission Unit

NGA Next Generation Access

NSA Non-Standalone

NTP Network Time Protocol

OI Outage Intensity

OSI Open Systems Interconnection

OT Operational Technology

PC Personal Computer

PDF Portable Document Format

PLR Packet Loss Rate

PQ Priority Queuing

PRBS Pseudo Random Binary Sequence

QAM Quadrature Amplitude Modulation

QoE Quality of Experience

QoS Quality of Services

RADIUS Remote Authentication Dial In User Service

RAN Radio Access Network

RED Random Early Detection

RFC Request For Comments

RFID Radio Frequency Identification

RSRP Reference Signal Receive Power

RSRQ Reference Signal Received Quality

RSSI Received Signal Strength Indication

RTL Real Time Location

RTT Round Trip Time

RWND Receive Window

SA Service Availability

SA Standalone

SCTP Stream Control Transmission Protocol

SIM Subscriber Identity Module

SINR Signal to Interference plus Noise Ratio

SLA Service Level Agreement

TCP Transmission Control Protocol

TDD Time Division Duplex

TP Throughput

UAS Unavailable Seconds

UDP User Datagram Protocol

URLLC Ultra Reliable and Low Latency

VBR Variable Bit Rate

VLAN Virtual Local Area Network

VoIP Voice over Internet Protocol

WFQ Weighted Fair Queuing

Wi-Fi Wireless Fidelity

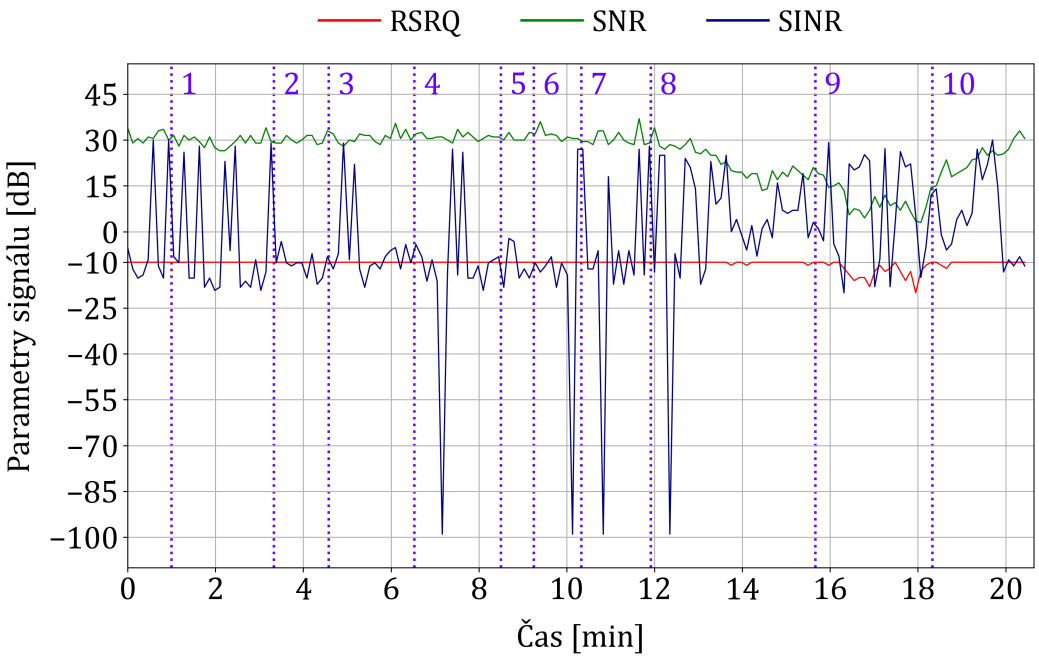
WPA Wi-Fi Protected Access

WRED Weighted Random Early Detection

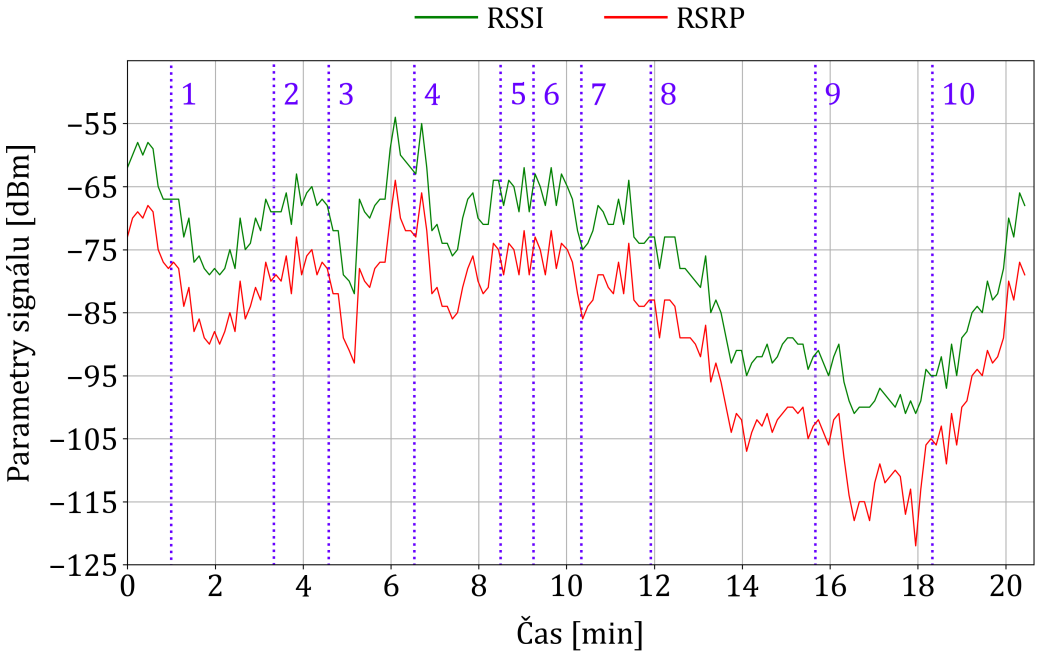
WWW World Wide Web

A. Příloha

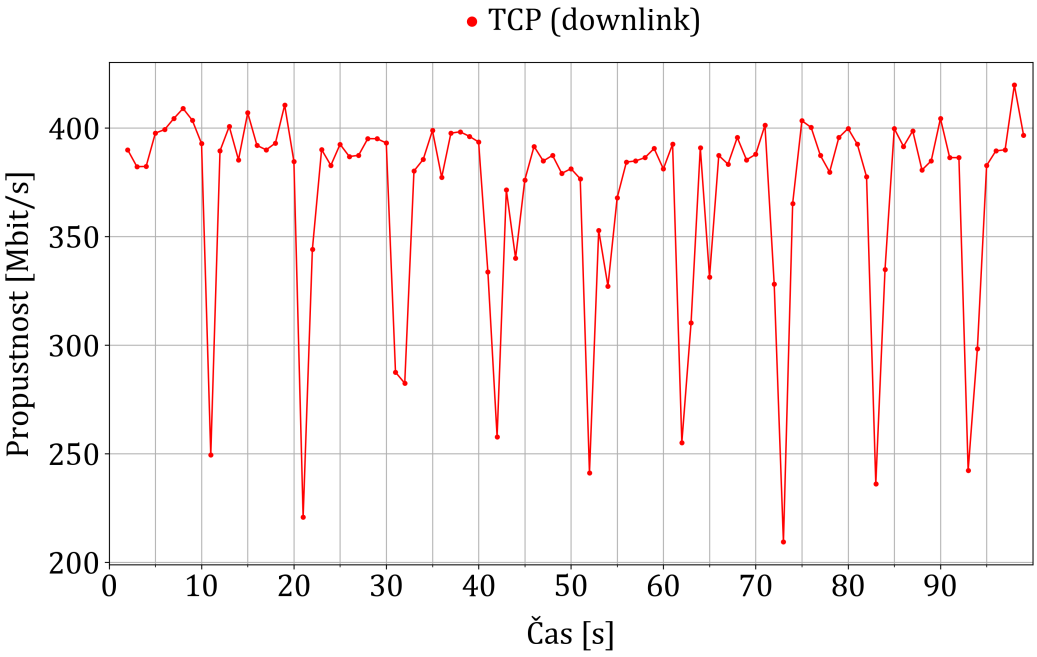
A.1 Grafy s výsledky prvotních testů



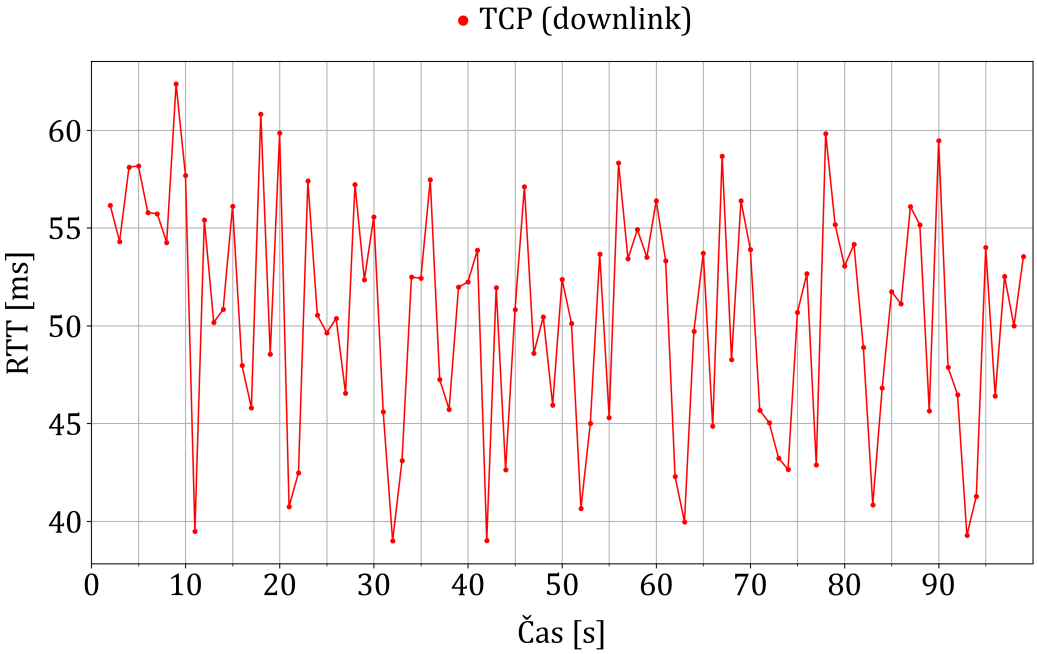
Obrázek A.1: Graf zobrazující RSRQ, SNR a SINR během testování za pohybu.



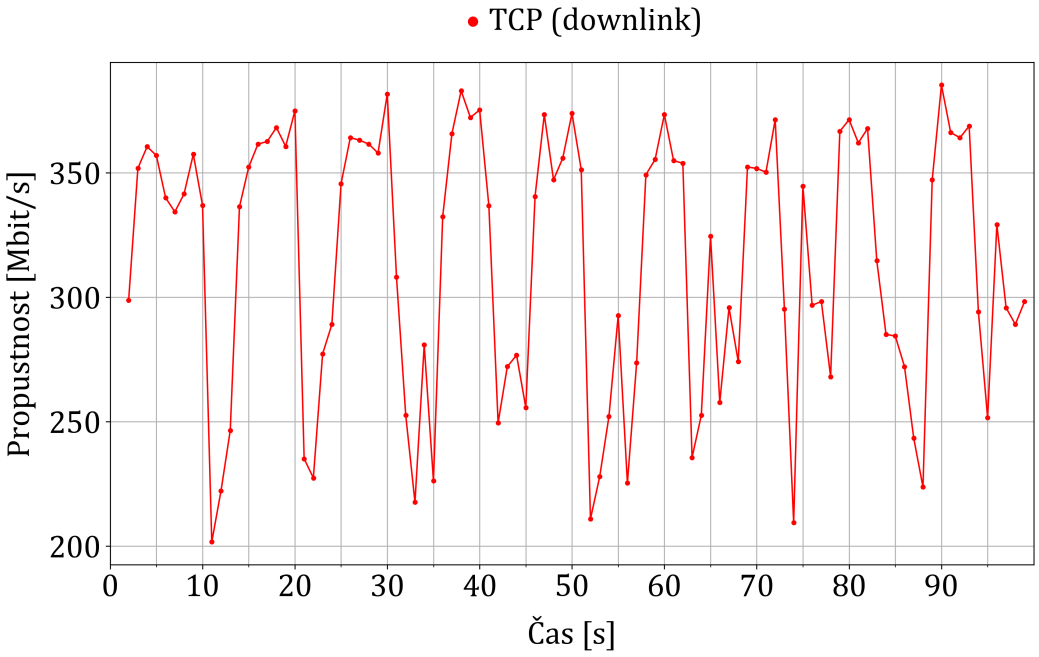
Obrázek A.2: Graf zobrazující RSSI a RSRP během testování za pohybu.



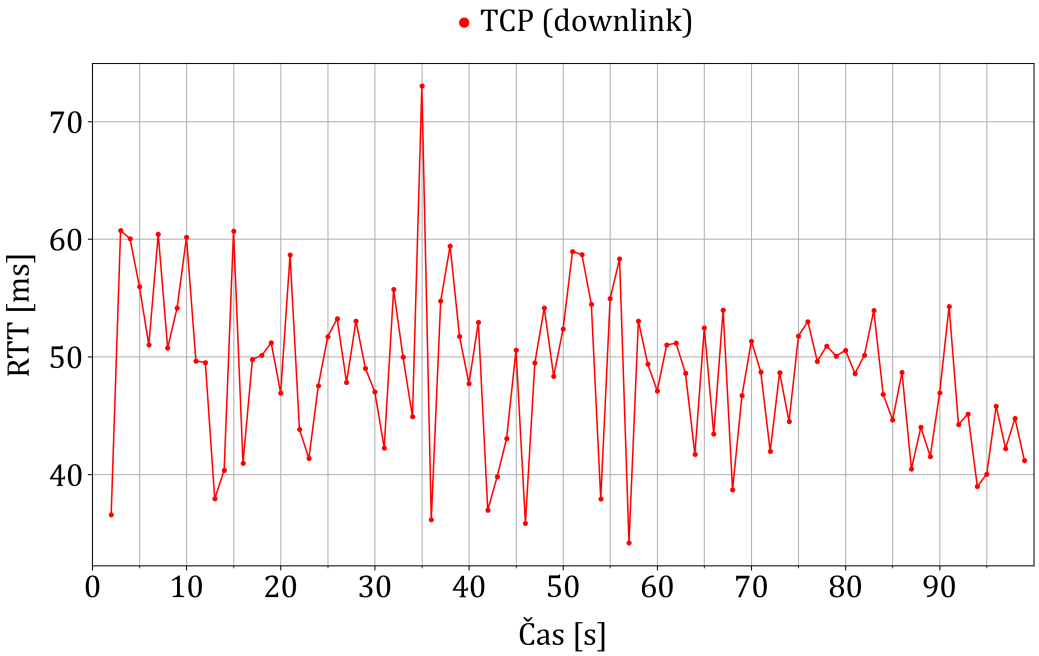
Obrázek A.3: Graf zobrazující naměřenou propustnost sítě scénářem 2A.



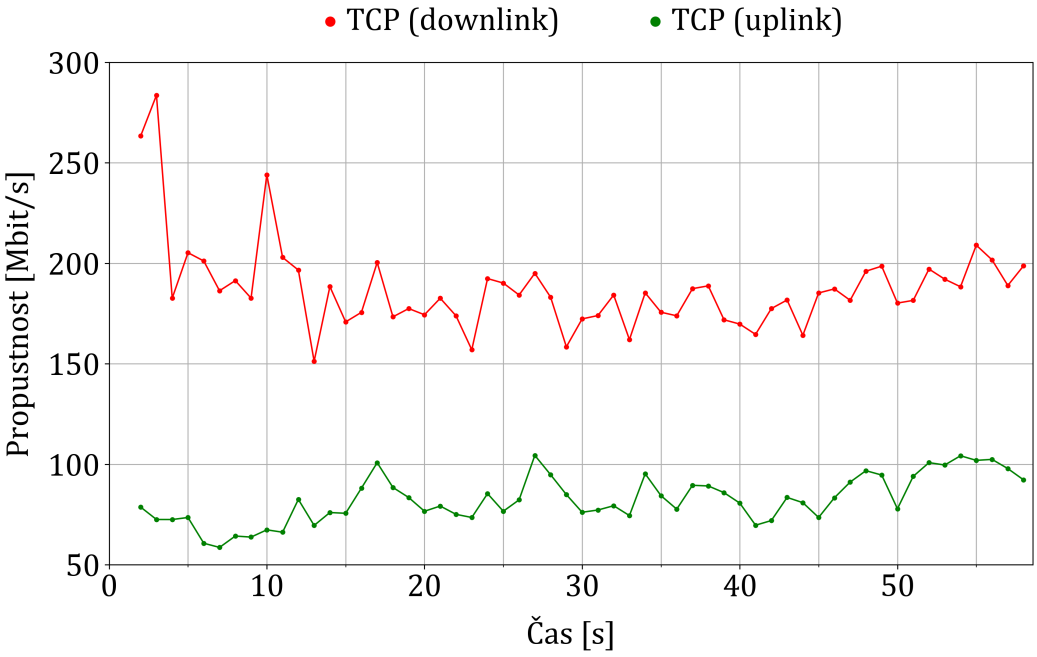
Obrázek A.4: Graf zobrazující naměřené RTT scénářem 2A.



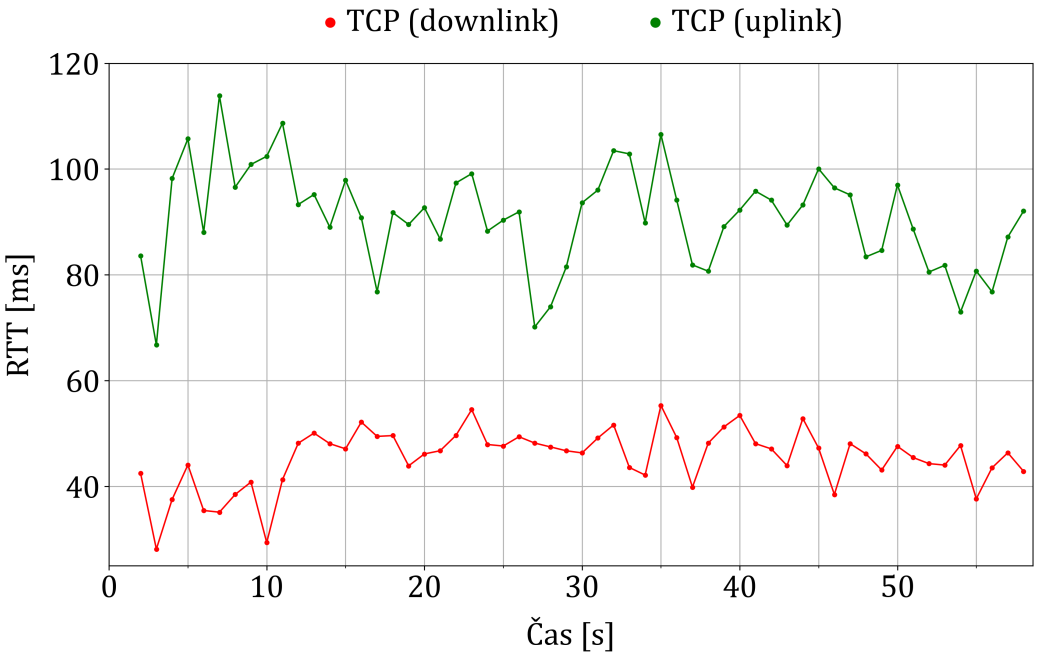
Obrázek A.5: Graf zobrazující naměřenou propustnost sítě scénářem 1B.



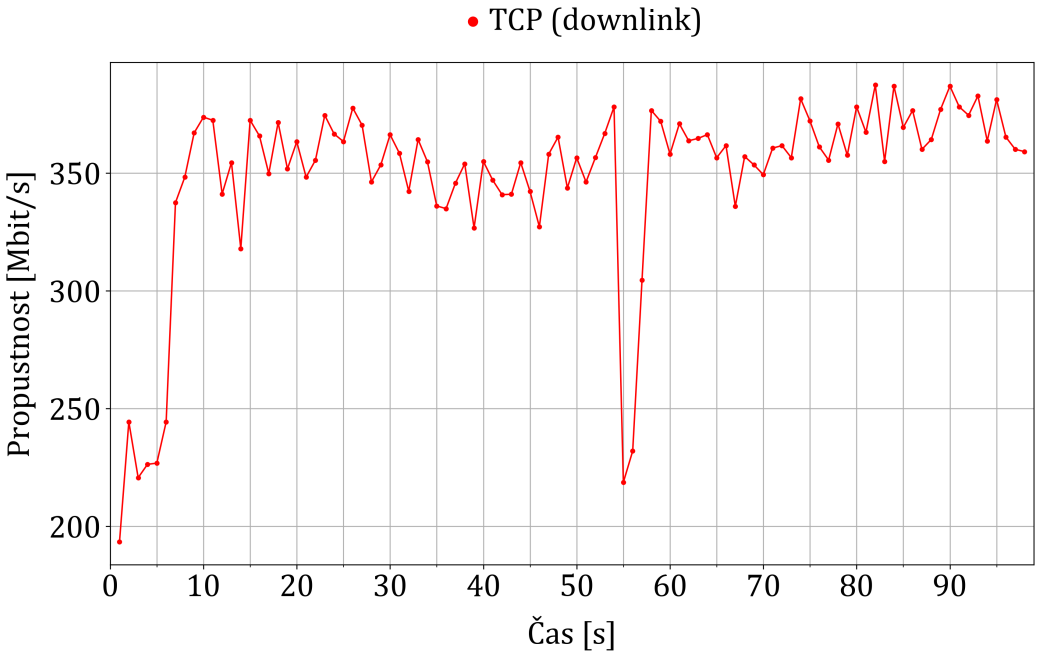
Obrázek A.6: Graf zobrazující naměřené RTT scénářem 1B.



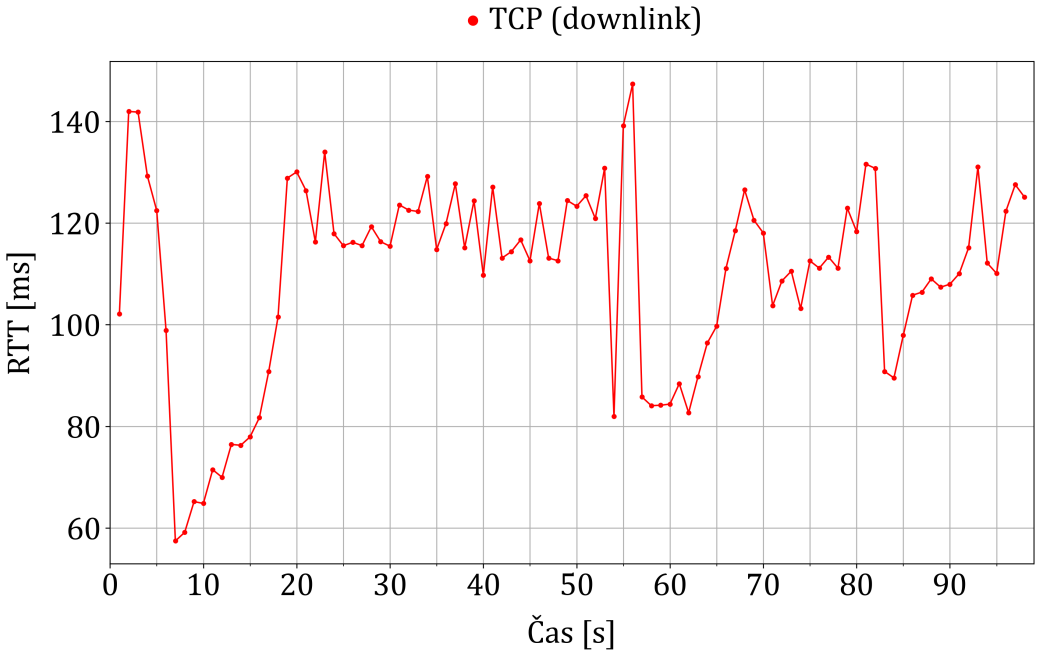
Obrázek A.7: Graf zobrazující naměřenou propustnost sítě scénářem 3B.



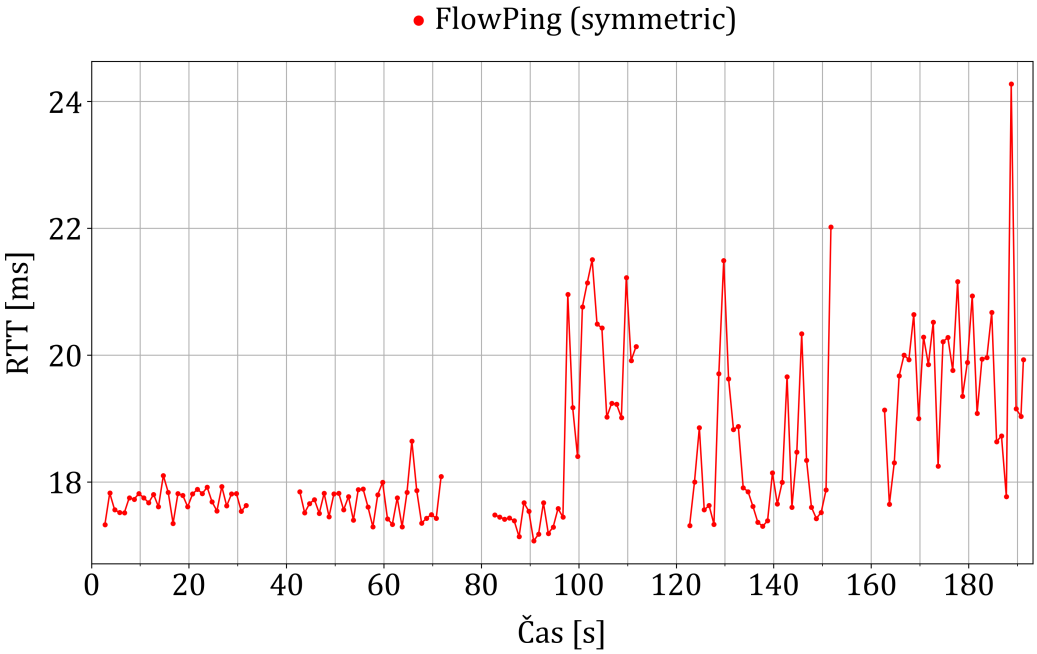
Obrázek A.8: Graf zobrazující naměřené RTT scénářem 3B.



Obrázek A.9: Graf zobrazující naměřenou propustnost sítě scénářem 4B.



Obrázek A.10: Graf zobrazující naměřené RTT scénářem 4B.



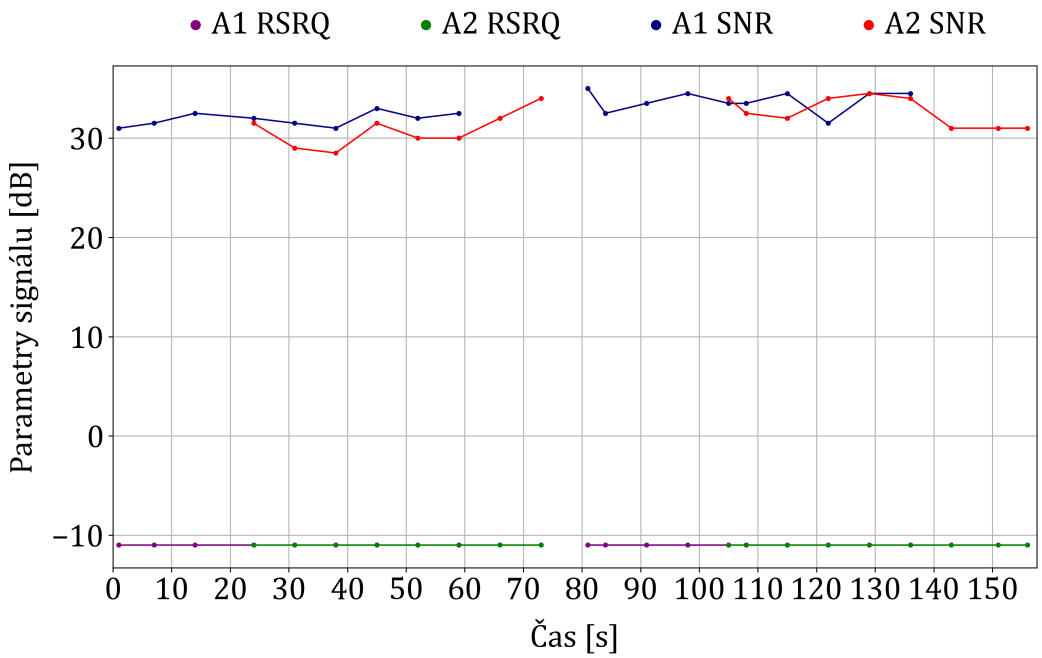
Obrázek A.11: Graf zobrazující naměřené RTT scénářem 2B (UDP toky, přenosová rychlost 10 Mbit/s a velikost paketů 1400 B).

A.2 Soubory obsahující naměřená data z prvotních testů

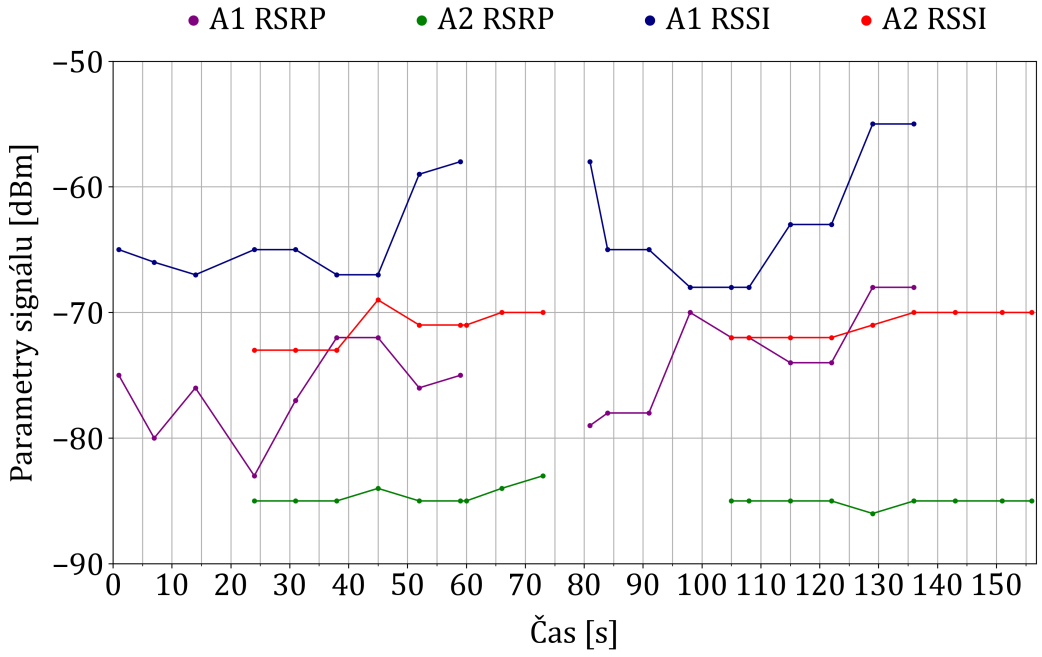
Součástí diplomové práce je složka s naměřenými daty. V této složce je podsložka s názvem `prvotni_testy`. Obsahuje soubory .pdf, .csv a .zip vygenerované platformou F-Tester v rámci prvotních testů.

B. Příloha

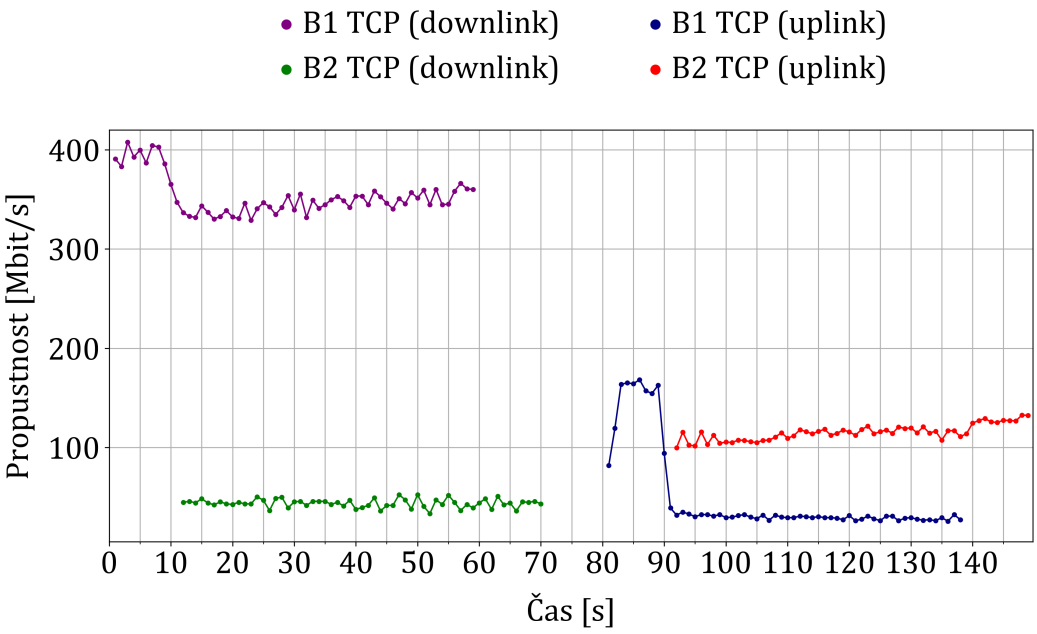
B.1 Grafy s výsledky vícebodových testů



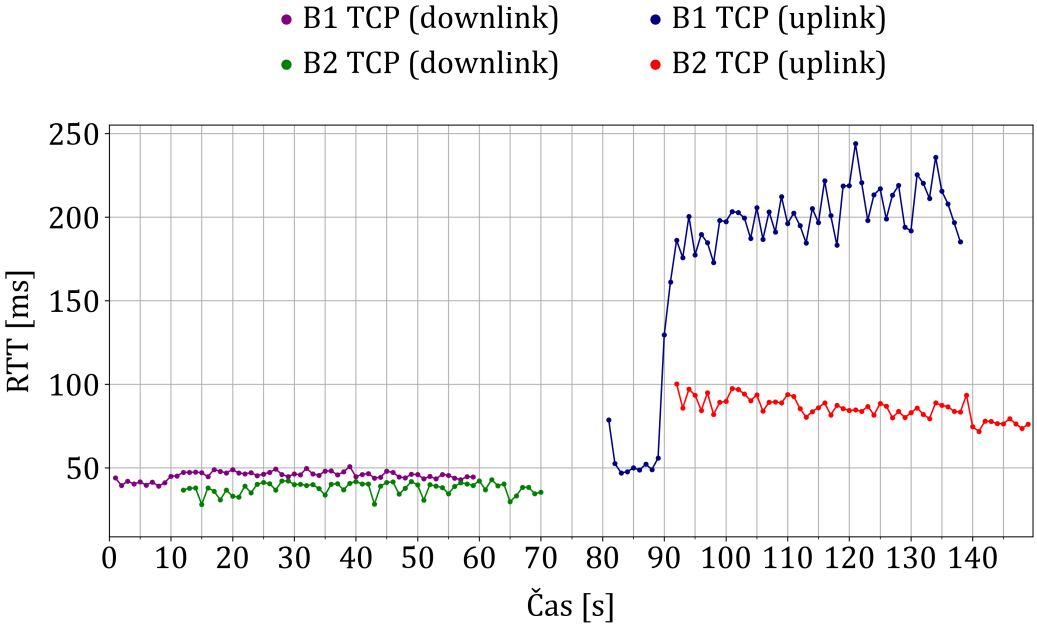
Obrázek B.1: Graf zobrazující naměřené RSRQ a SNR scénářem A1 (pohyb z bodu X do bodu Y a zpět do bodu X) a A2.



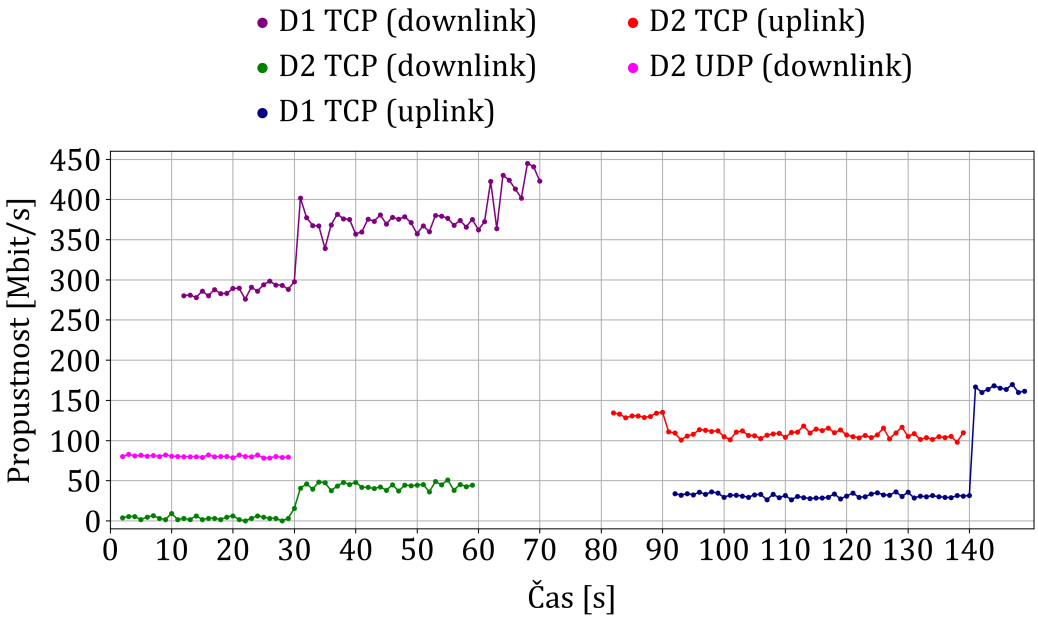
Obrázek B.2: Graf zobrazující naměřené RSRP a RSSI scénářem A1 (pohyb z bodu X do bodu Y a zpět do bodu X) a A2.



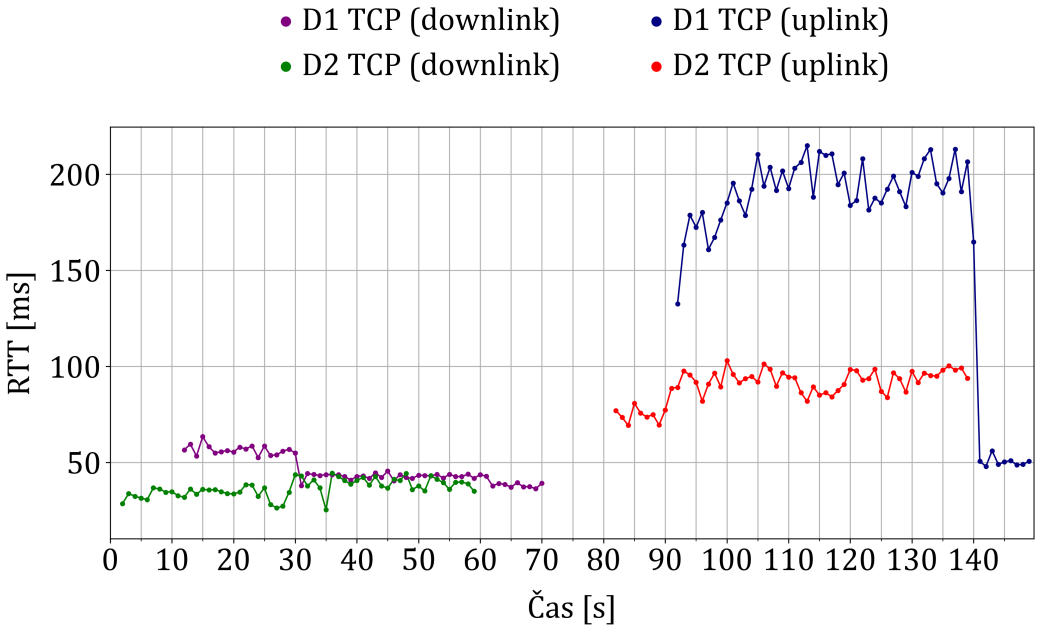
Obrázek B.3: Graf zobrazující naměřenou propustnost sítě scénářem B1 (pohyb z bodu Y do bodu X) a B2.



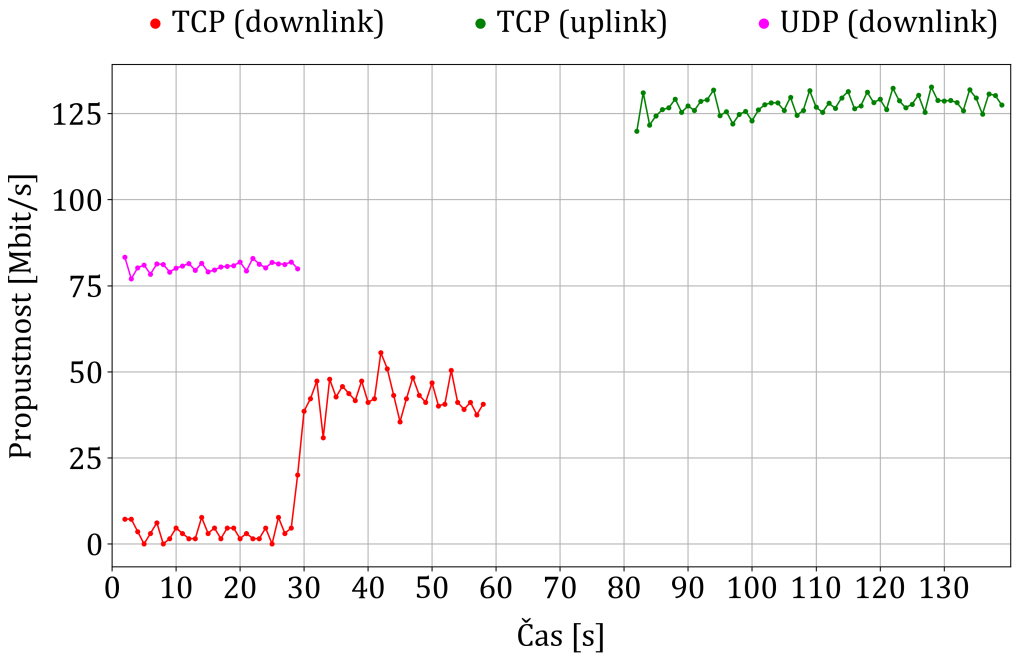
Obrázek B.4: Graf zobrazující naměřené RTT scénářem B1 (pohyb z bodu Y do bodu X) a B2.



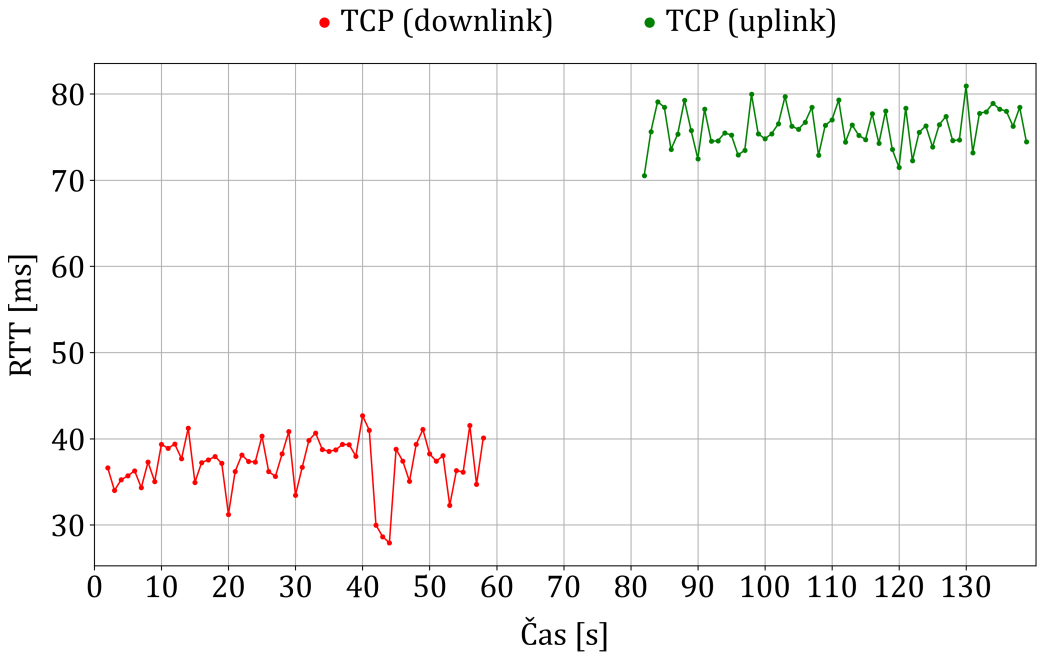
Obrázek B.5: Graf zobrazující naměřenou propustnost sítě scénářem D1 (pohyb z bodu X do bodu Y a zpět do bodu X) a D2.



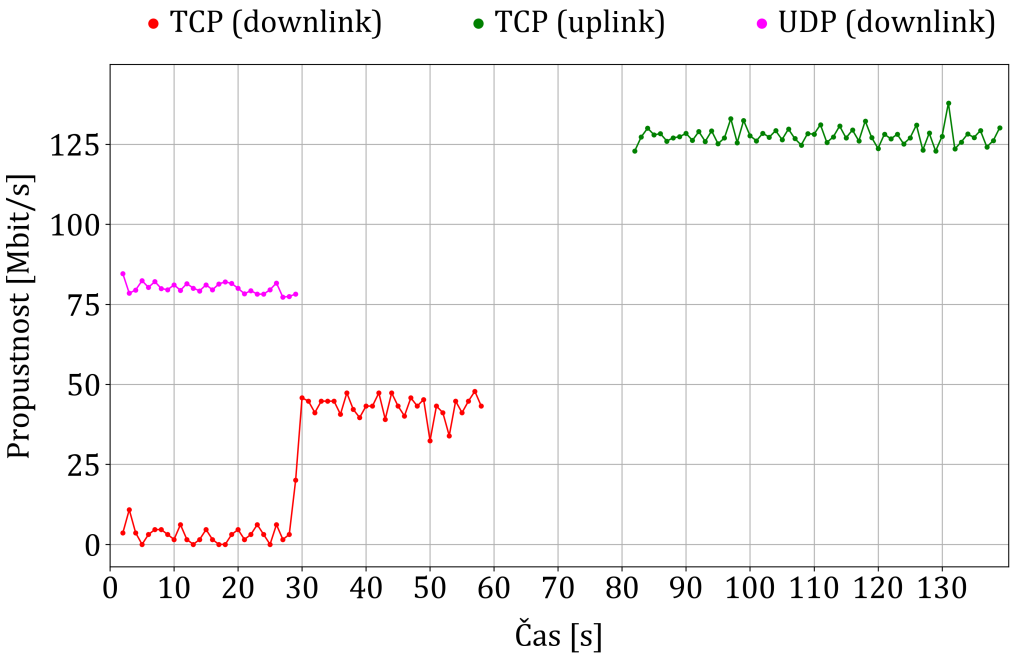
Obrázek B.6: Graf zobrazující naměřené RTT scénářem D1 (pohyb z bodu X do bodu Y a zpět do bodu X) a D2.



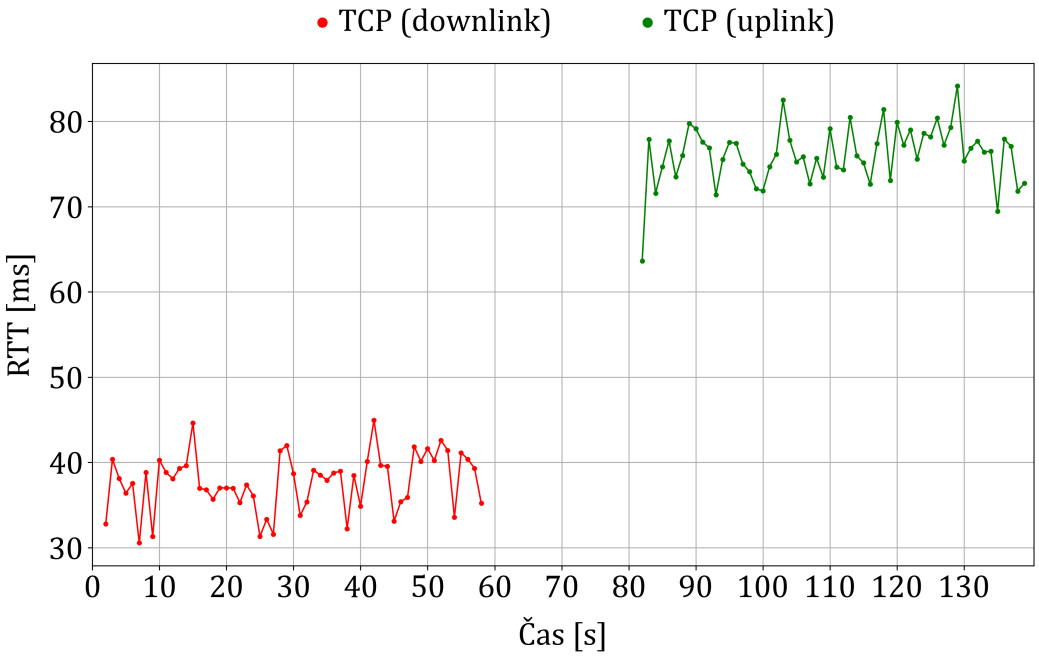
Obrázek B.7: Graf zobrazující naměřenou propustnost sítě scénářem Y2, který byl spuštěn po odpojení F-Testeru 5G (pohyblivý) z privátní sítě 5G.



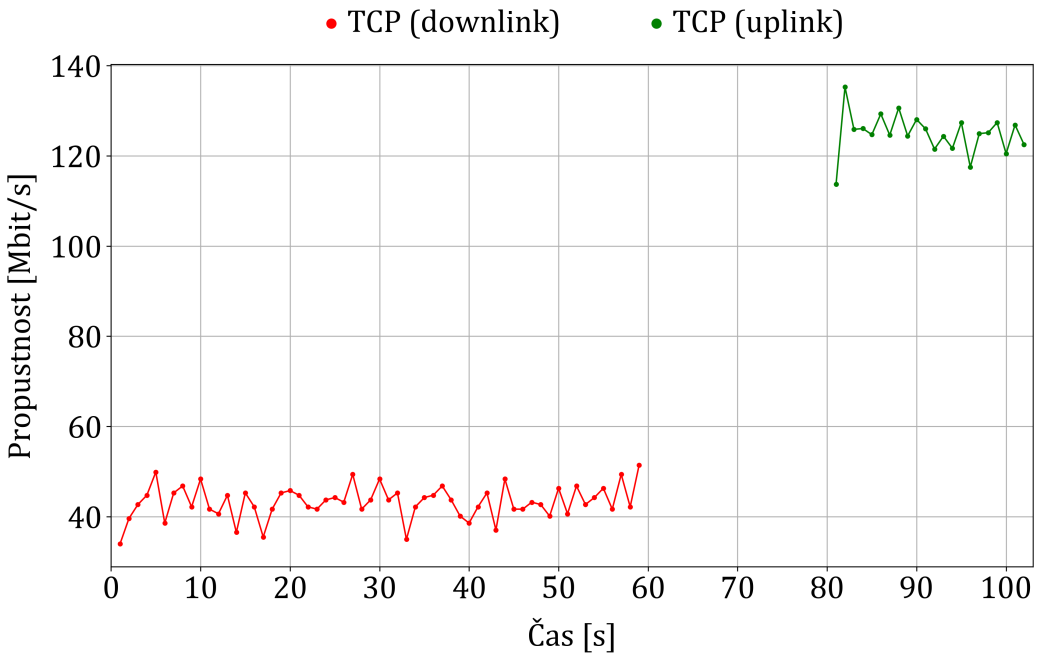
Obrázek B.8: Graf zobrazující naměřené RTT scénářem Y2, který byl spuštěn po odpojení F-Testeru 5G (pohyblivý) z privátní sítě 5G.



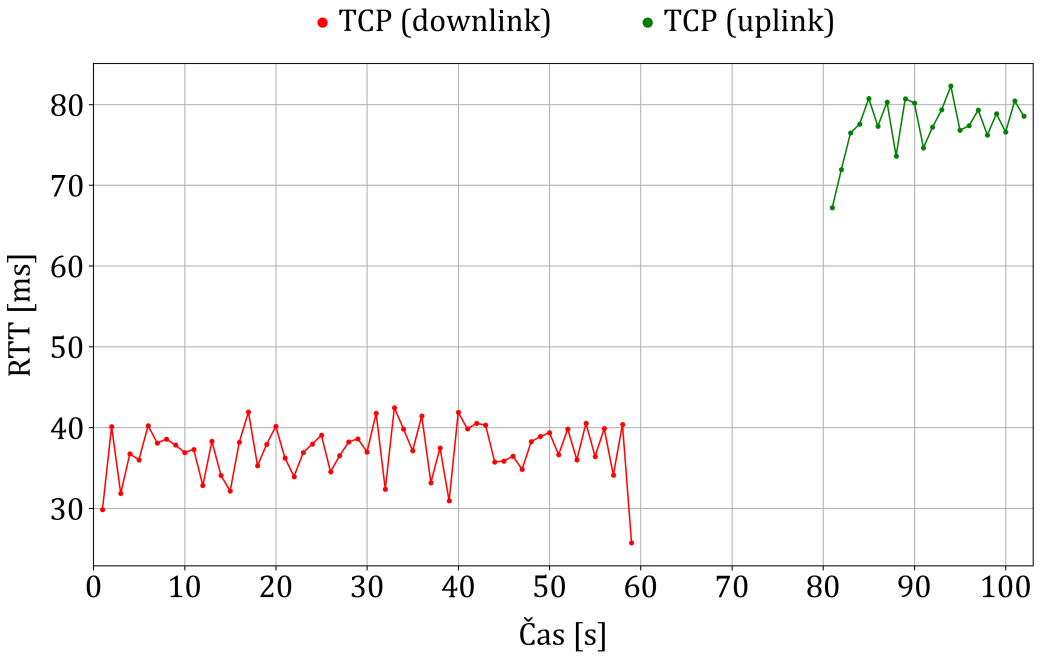
Obrázek B.9: Graf zobrazující naměřenou propustnost sítě scénářem X2, který byl spuštěn po odpojení a následném připojení F-Testeru 5G (fixní) k privátní síti 5G.



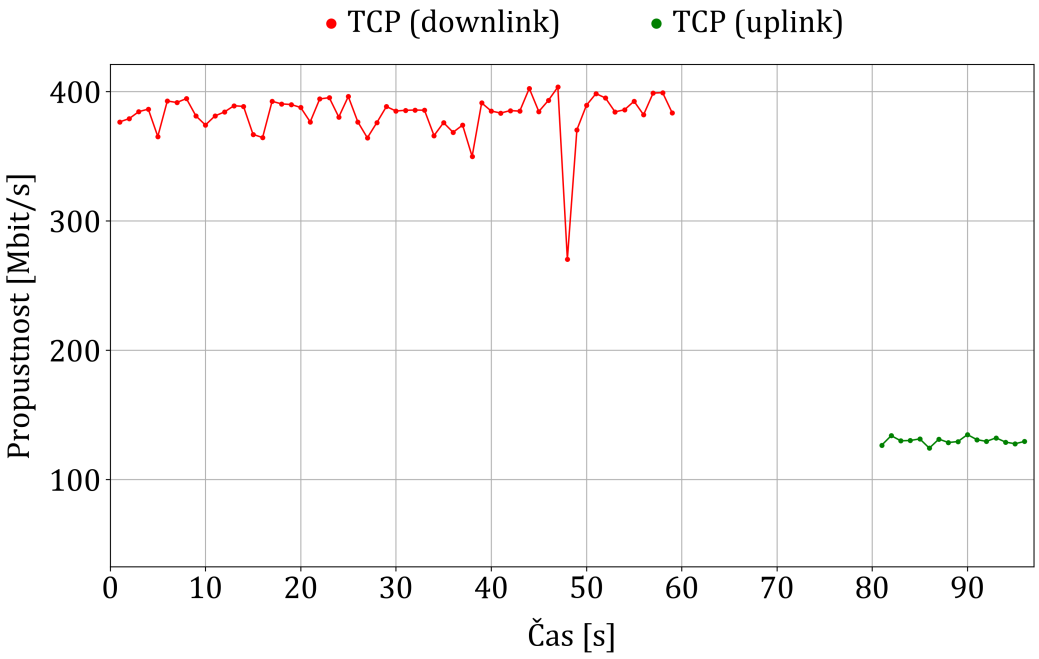
Obrázek B.10: Graf zobrazující naměřené RTT scénářem X2, který byl spuštěn po odpojení a následném připojení F-Testeru 5G (fixní) k privátní síti 5G.



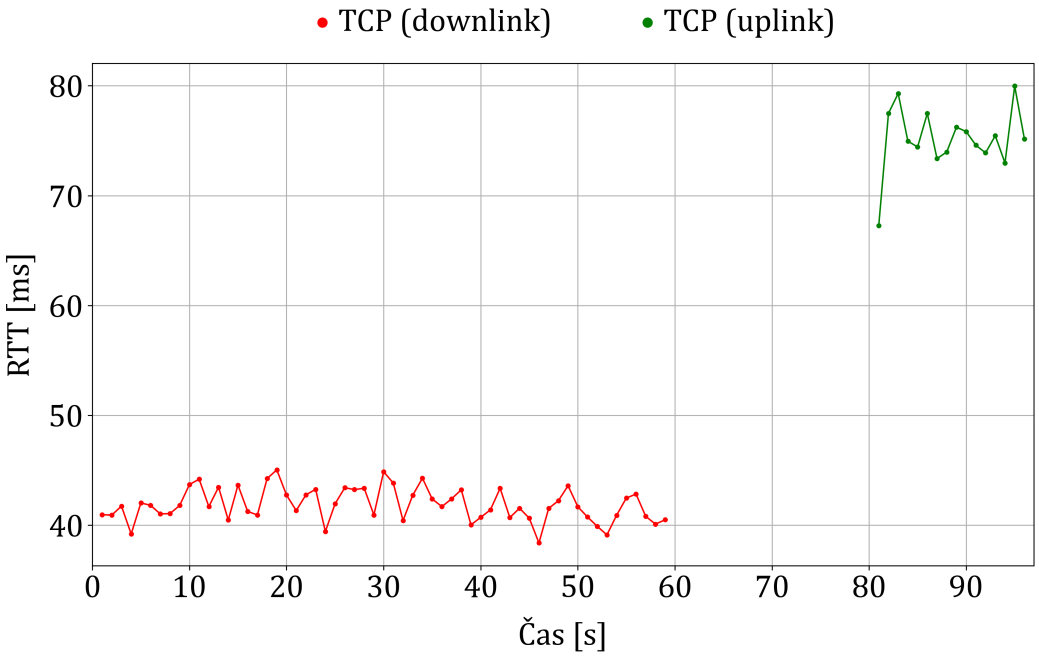
Obrázek B.11: Graf zobrazující naměřenou propustnost sítě scénářem W2, kdy byl F-Tester 5G (fixní) odpojen.



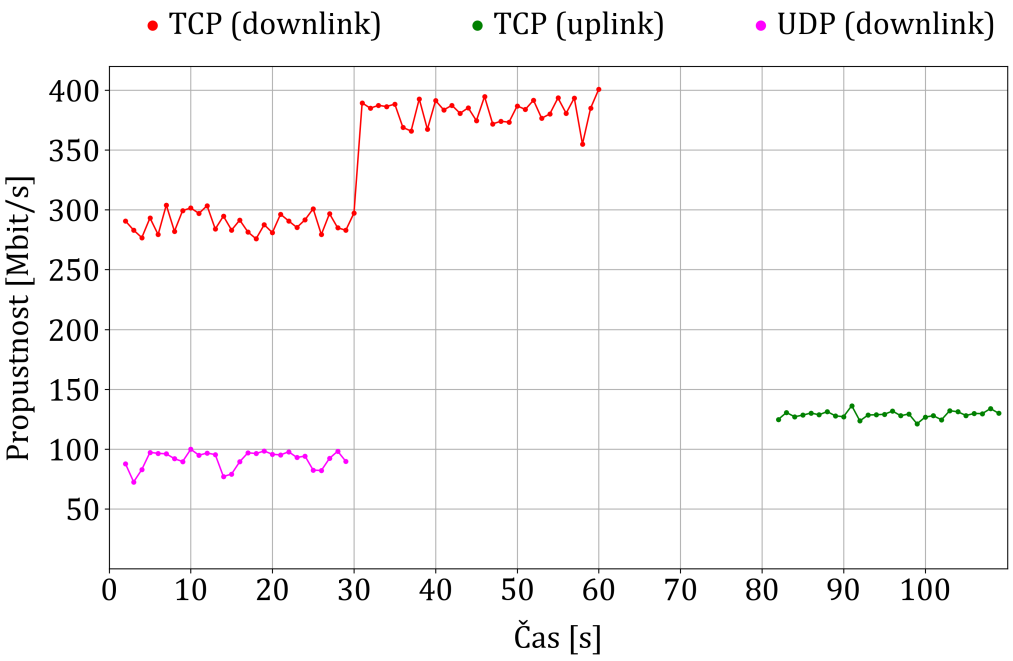
Obrázek B.12: Graf zobrazující naměřené RTT scénářem W2, kdy byl F-Tester 5G (fixní) odpojen.



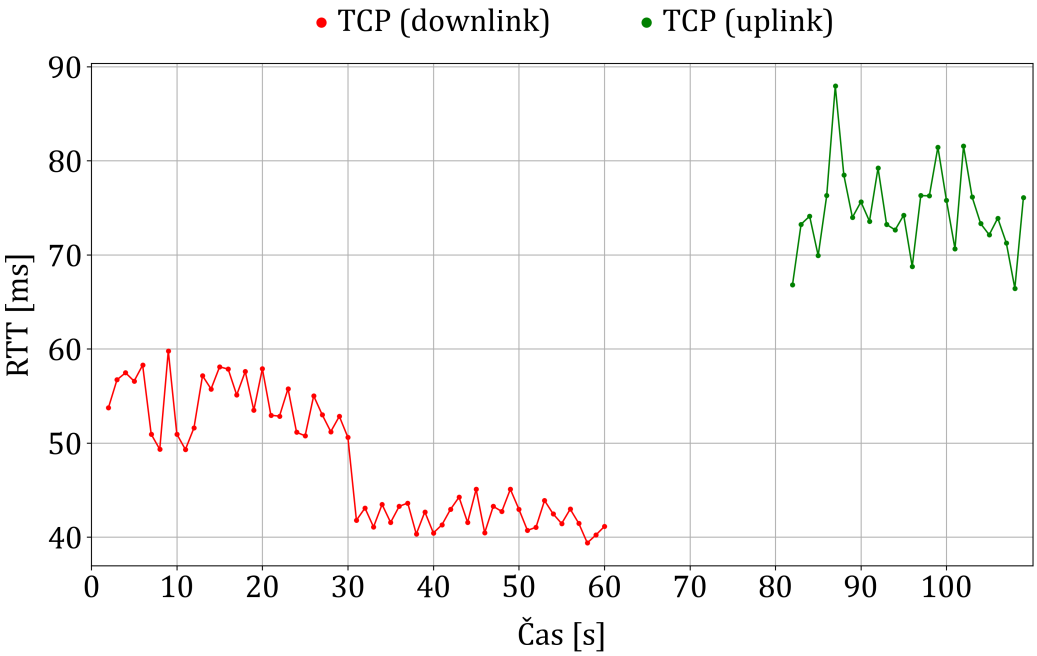
Obrázek B.13: Graf zobrazující naměřenou propustnost sítě scénářem U2, kdy před jeho spuštěním byl F-Tester 5G (fixní) po restartu.



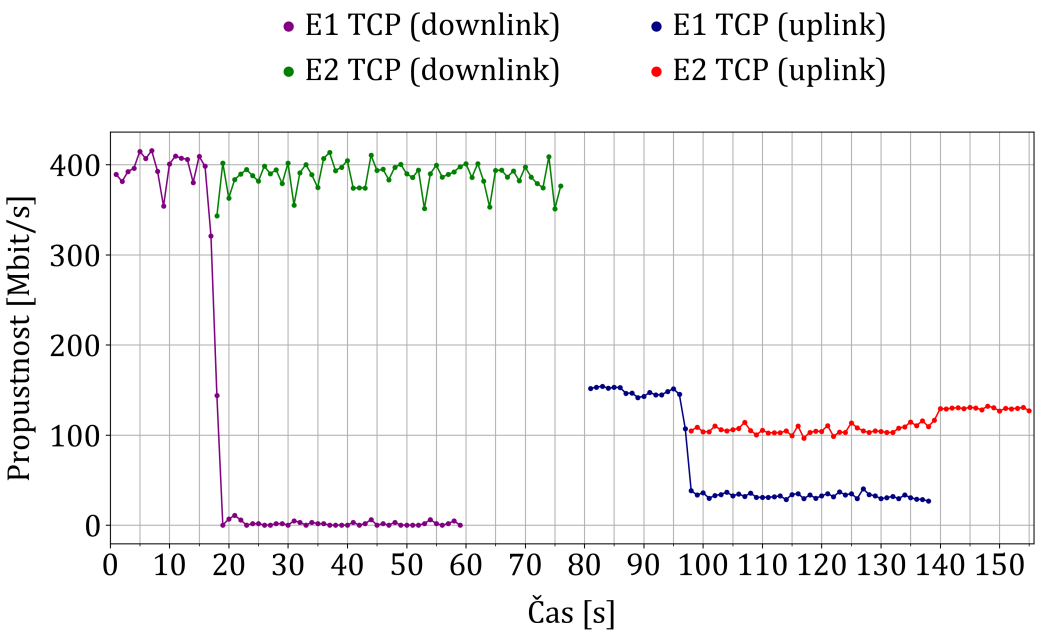
Obrázek B.14: Graf zobrazující naměřené RTT scénářem U2, kdy před jeho spuštěním byl F-Tester 5G (fixní) po restartu.



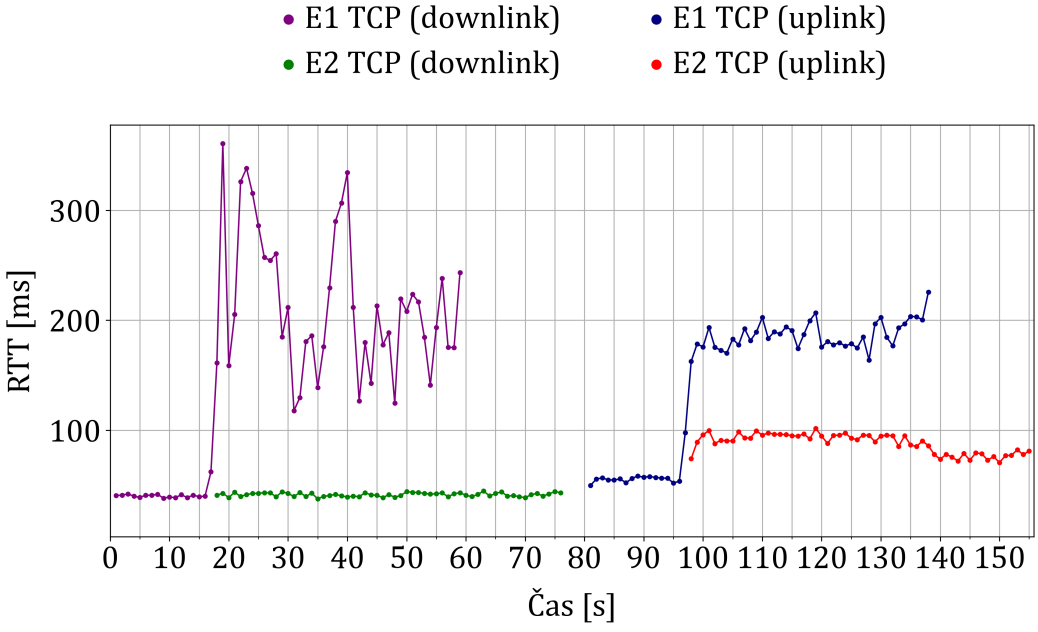
Obrázek B.15: Graf zobrazující naměřenou propustnost sítě scénářem T2.



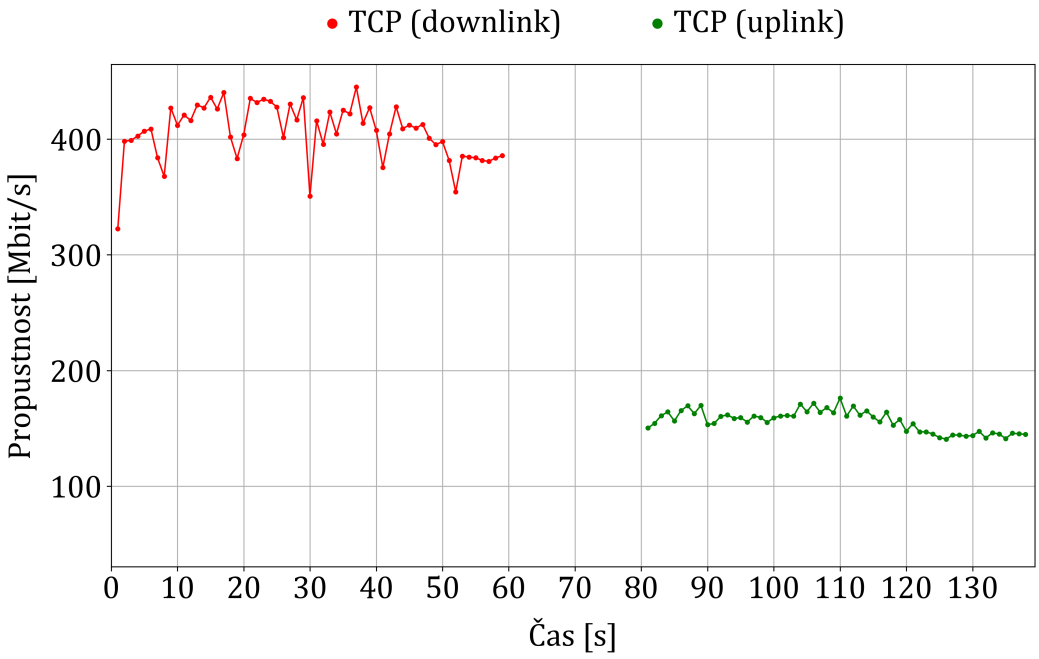
Obrázek B.16: Graf zobrazující naměřené RTT scénářem T2.



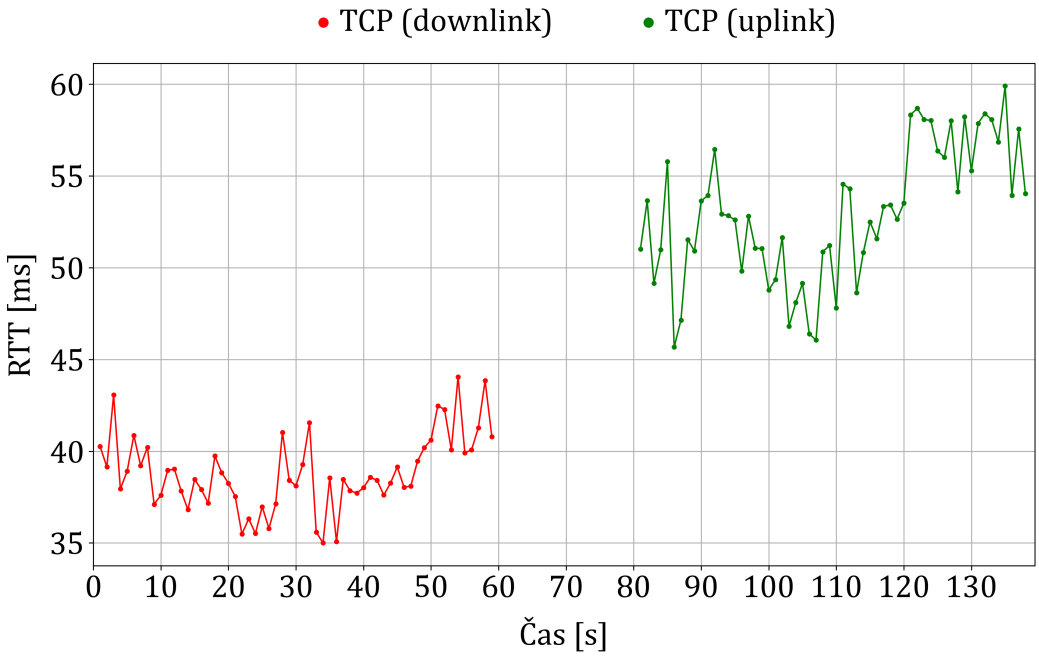
Obrázek B.17: Graf zobrazující naměřenou propustnost sítě scénářem E1 (pohyb z bodu X do bodu Y a zpět do bodu X) a E2.



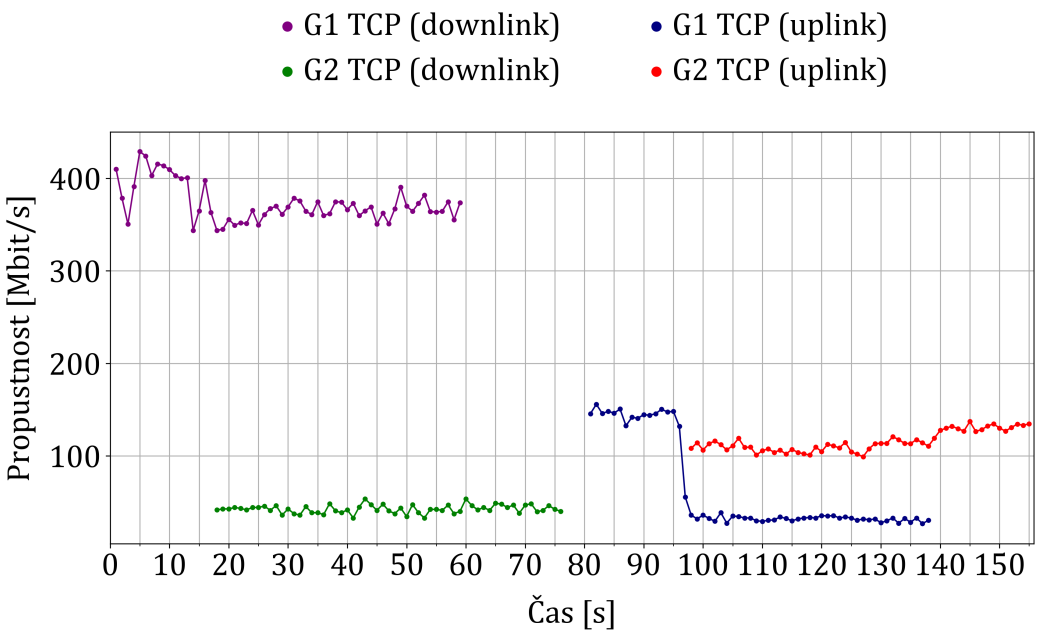
Obrázek B.18: Graf zobrazující naměřené RTT scénářem E1 (pohyb z bodu X do bodu Y a zpět do bodu X) a E2.



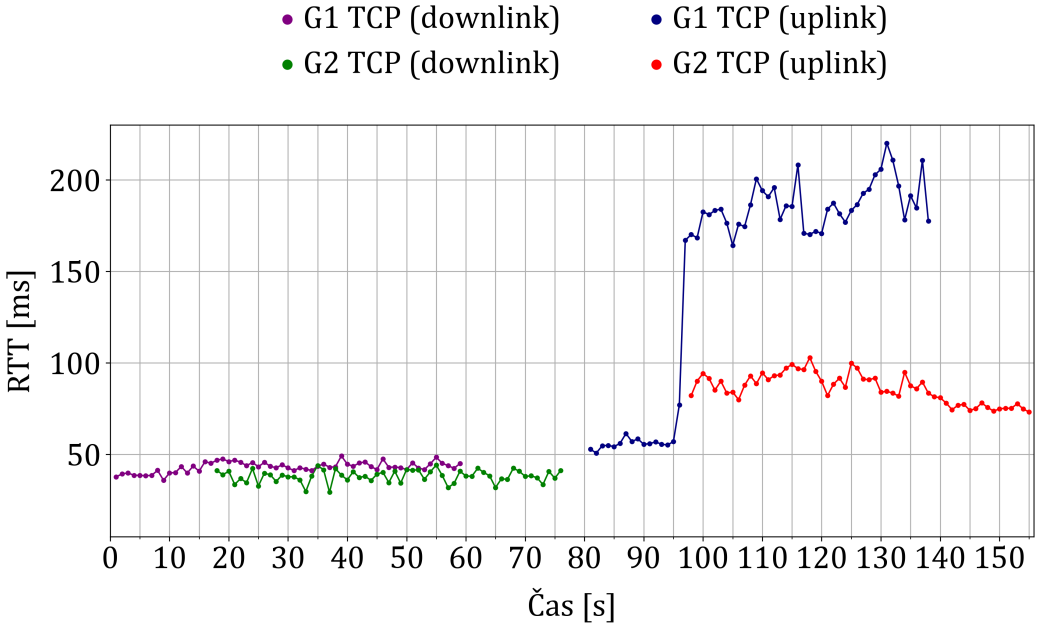
Obrázek B.19: Graf zobrazující naměřenou propustnost scénářem F1, který byl spuštěn při neaktivním F-Testeru 5G (fixní).



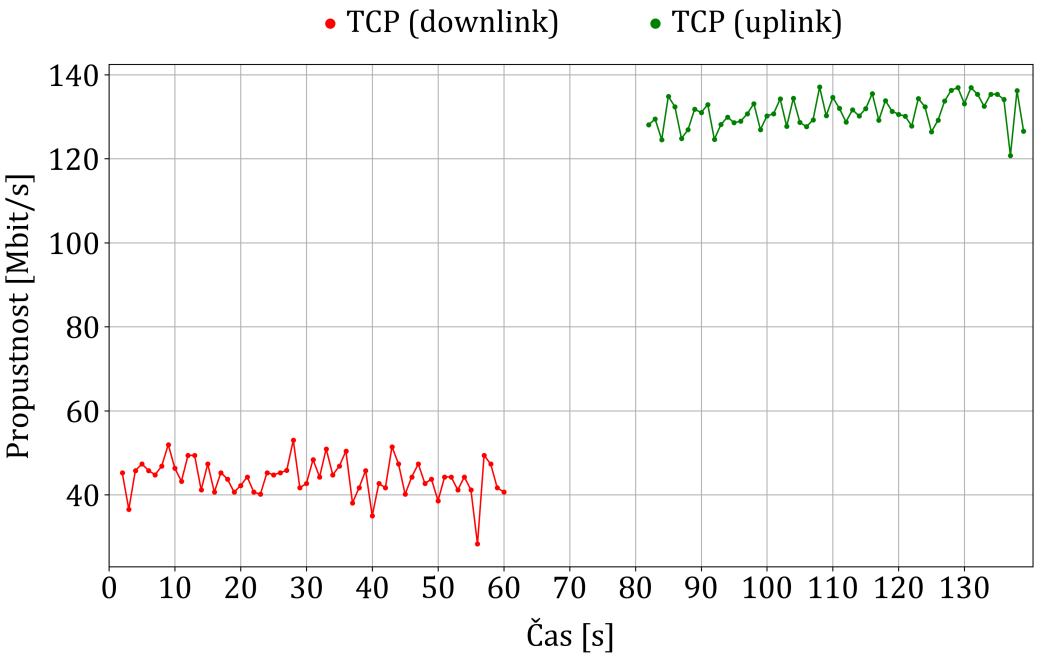
Obrázek B.20: Graf zobrazující naměřené RTT scénářem F1, který byl spuštěn při neaktivním F-Testeru 5G (fixní).



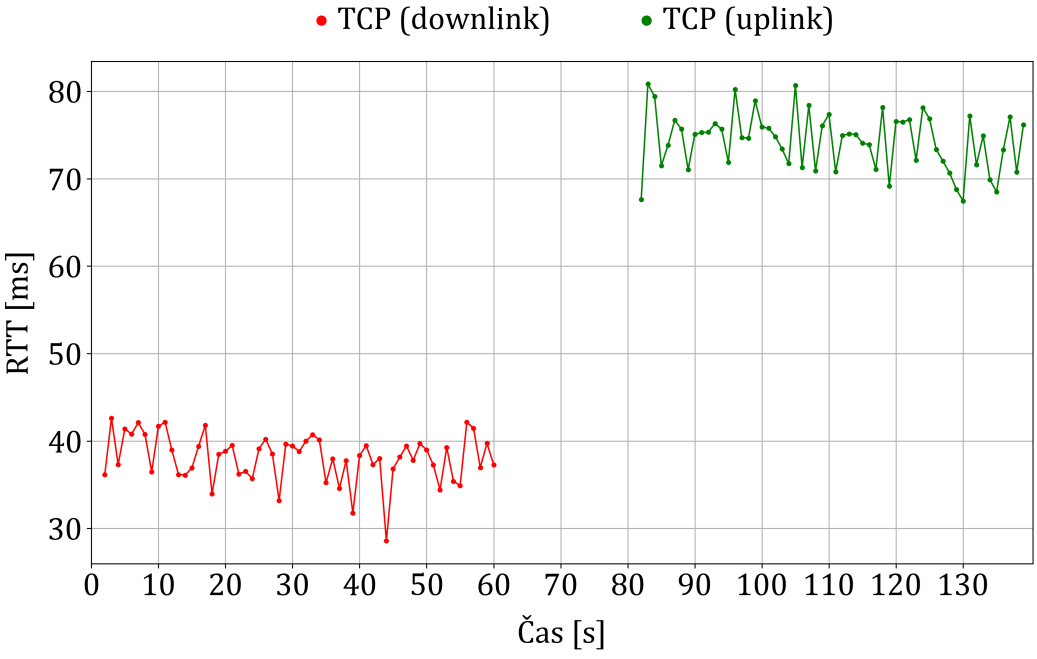
Obrázek B.21: Graf zobrazující naměřenou propustnost sítě scénářem G1 (pohyb z bodu X do bodu Y a zpět do bodu X) a G2.



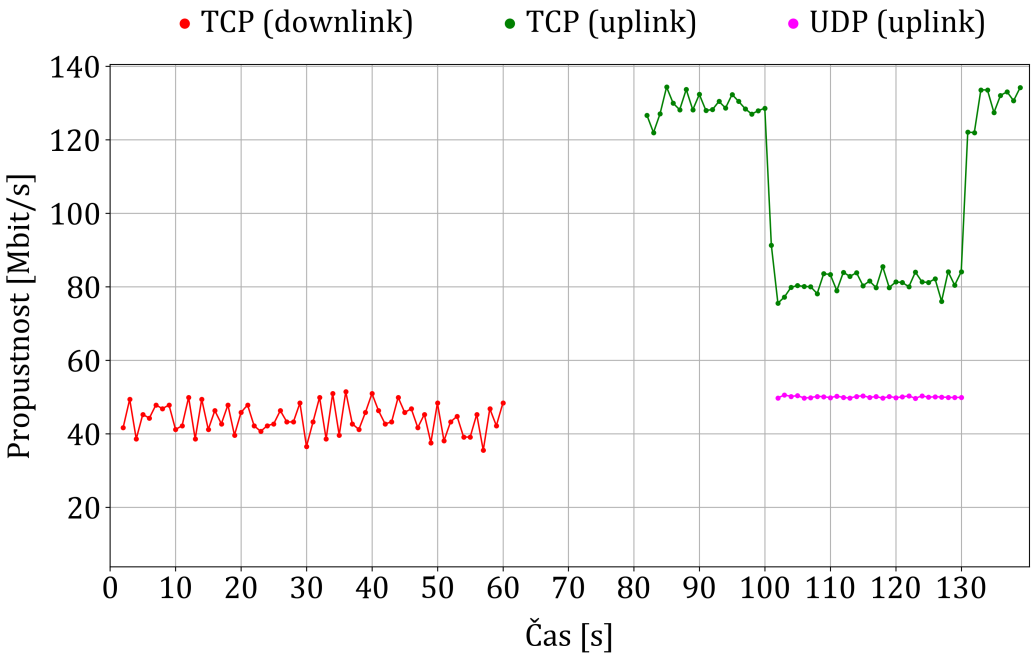
Obrázek B.22: Graf zobrazující naměřené RTT scénářem G1 (pohyb z bodu X do bodu Y a zpět do bodu X) a G2.



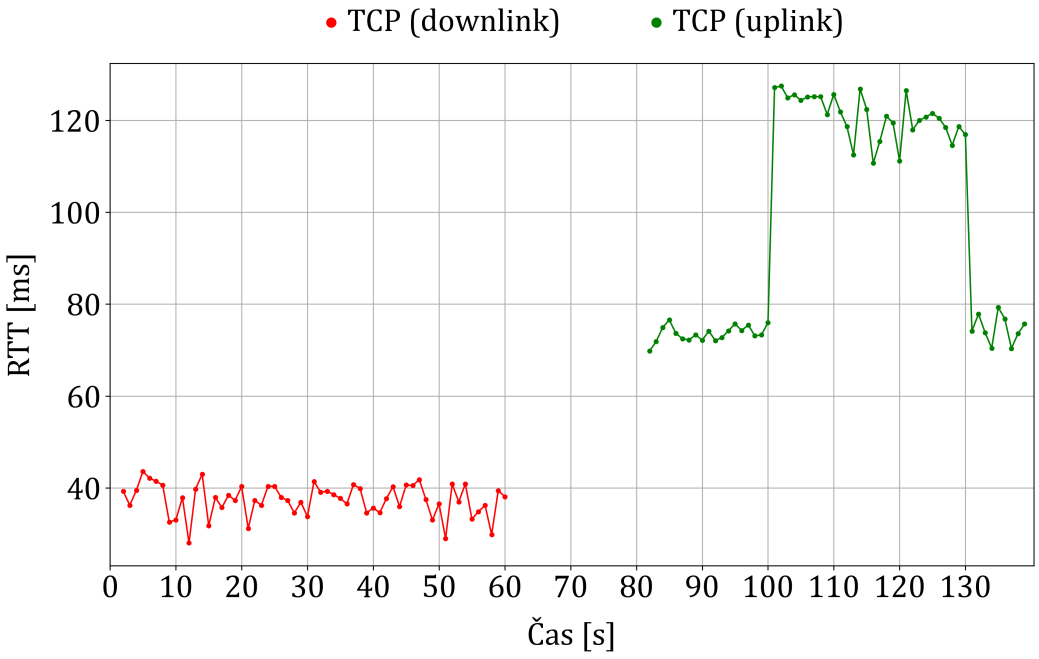
Obrázek B.23: Graf zobrazující naměřenou propustnost scénářem S2, který byl spuštěn při neaktivním F-Testeru 5G (pohyblivý).



Obrázek B.24: Graf zobrazující naměřené RTT scénářem S2, který byl spuštěn při neaktivním F-Testeru 5G (pohyblivý).

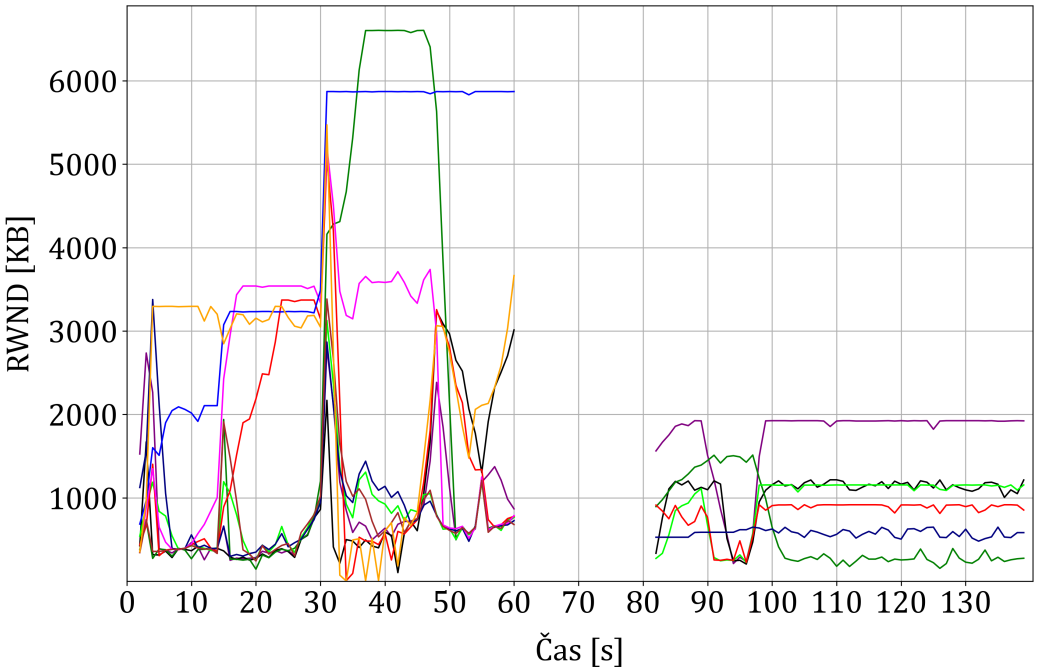


Obrázek B.25: Graf zobrazující naměřenou propustnost scénářem R2, který byl spuštěn při neaktivním F-Testeru 5G (pohyblivý).

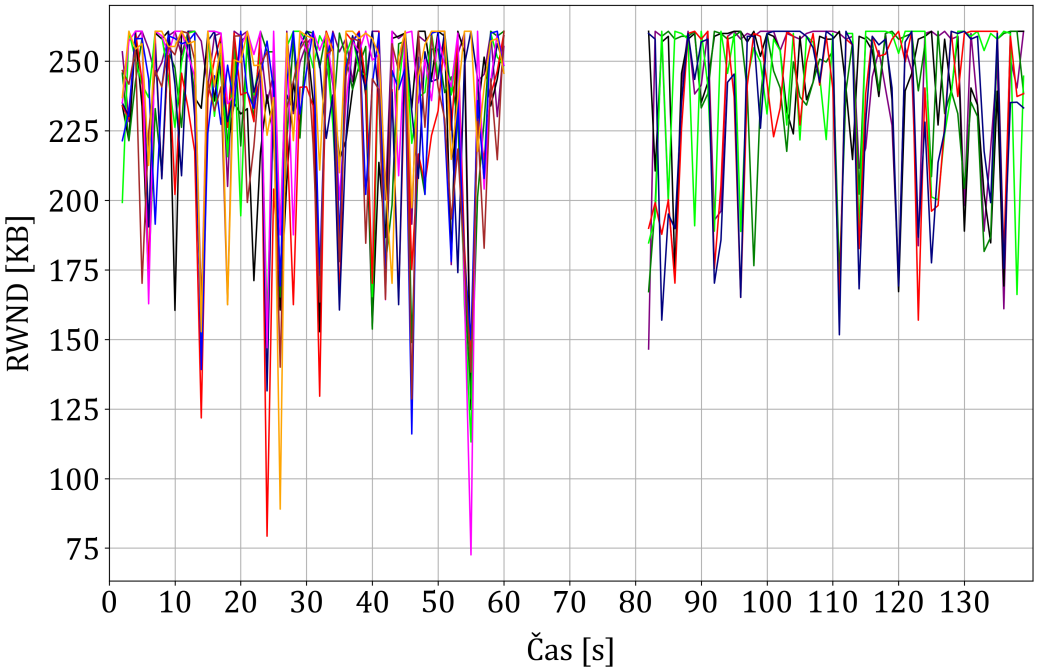


Obrázek B.26: Graf zobrazující naměřené RTT scénářem R2, který byl spuštěn při neaktivním F-Testeru 5G (pohyblivý).

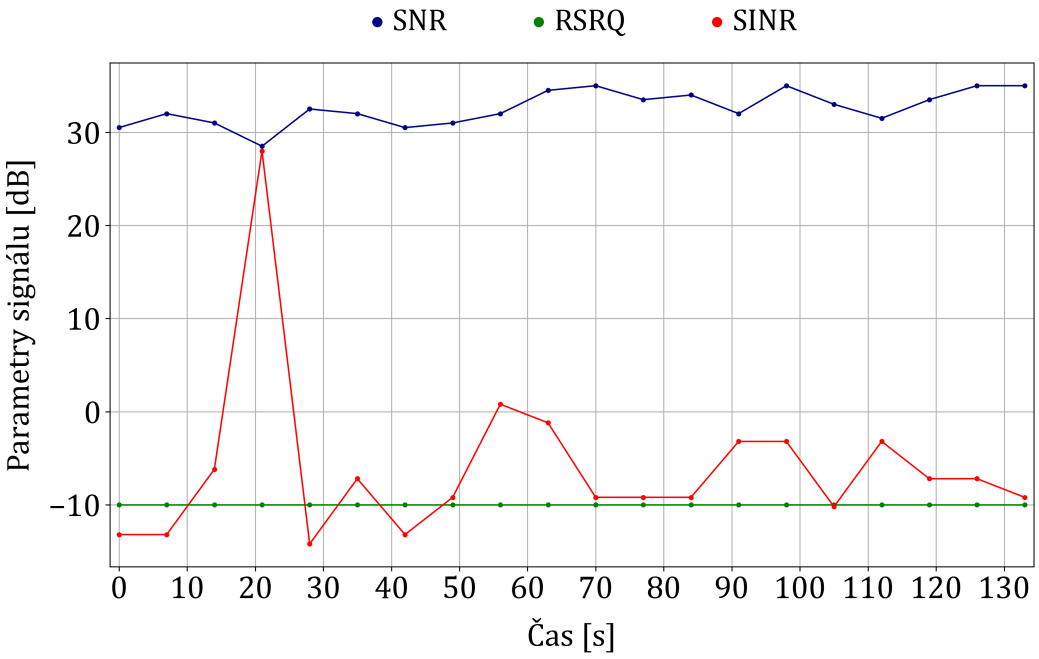
B.2 Grafy zobrazující výstupy z testování automatického TCP okna



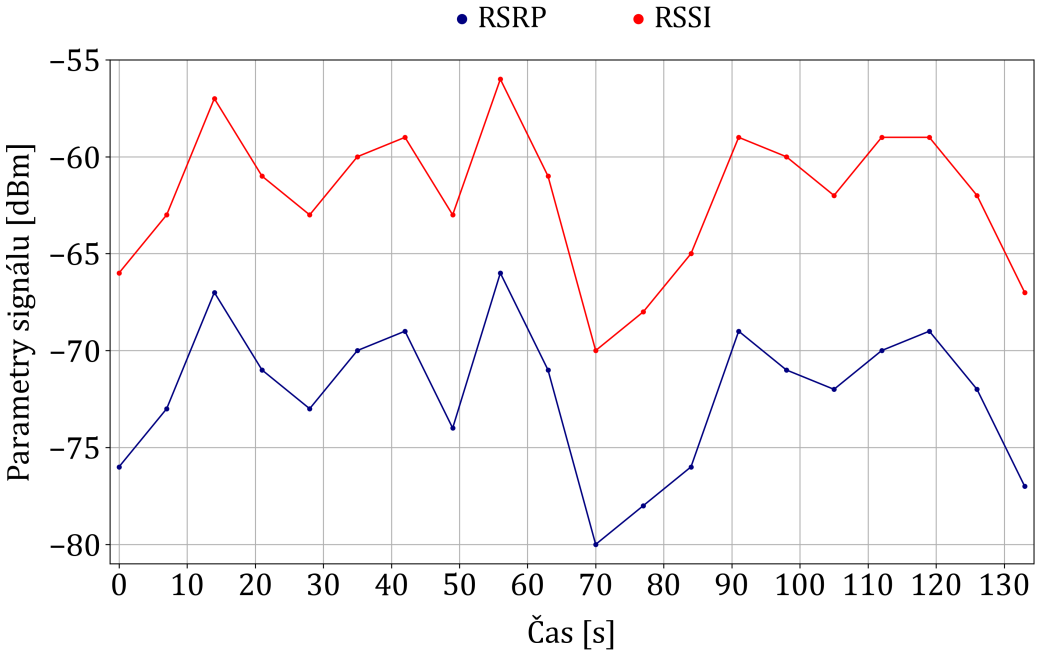
Obrázek B.27: Graf zobrazující rozmezí hodnot RWND během spuštěného scénáře N1 (pohyb z bodu A do bodu B a zpět do bodu A) pro 10 TCP toků (downlink, 0 až 60 s) a 6 TCP toků (uplink, 80 až 140 s).



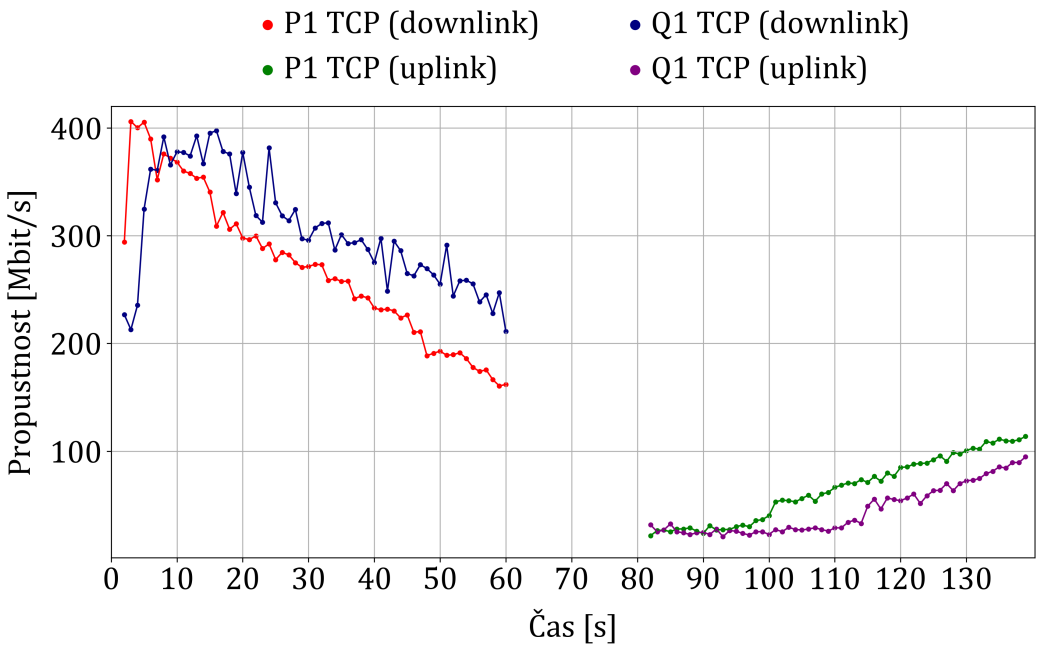
Obrázek B.28: Graf zobrazující rozmezí hodnot RWND během spuštěného scénáře O1 (pohyb z bodu A do bodu B a zpět do bodu A) pro 10 TCP toků (downlink, 0 až 60 s) a 6 TCP toků (uplink, 80 až 140 s).



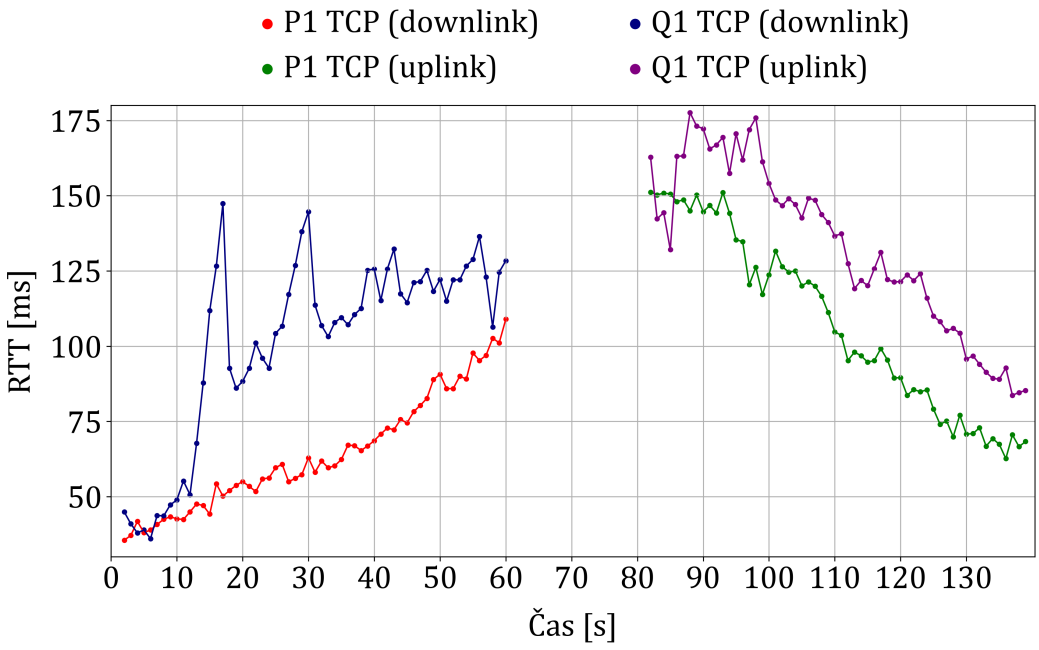
Obrázek B.29: Graf zobrazující naměřené SNR, RSRQ a SINR scénářem N1 (pohyb z bodu A do bodu B a zpět do bodu A).



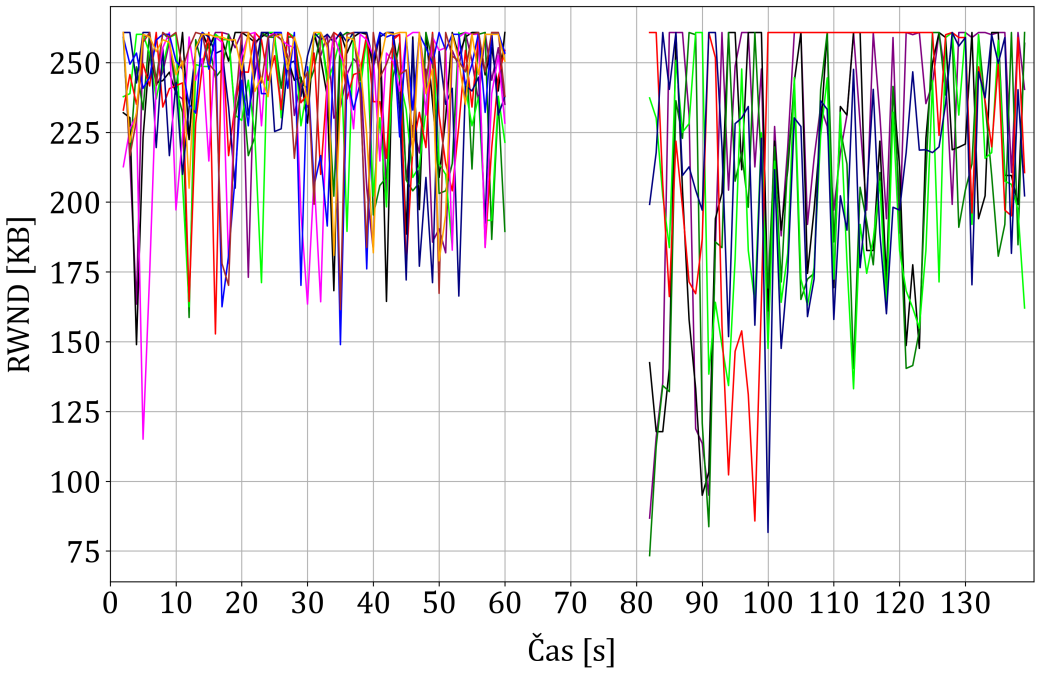
Obrázek B.30: Graf zobrazující naměřené RSRP a RSSI scénářem N1 (pohyb z bodu A do bodu B a zpět do bodu A).



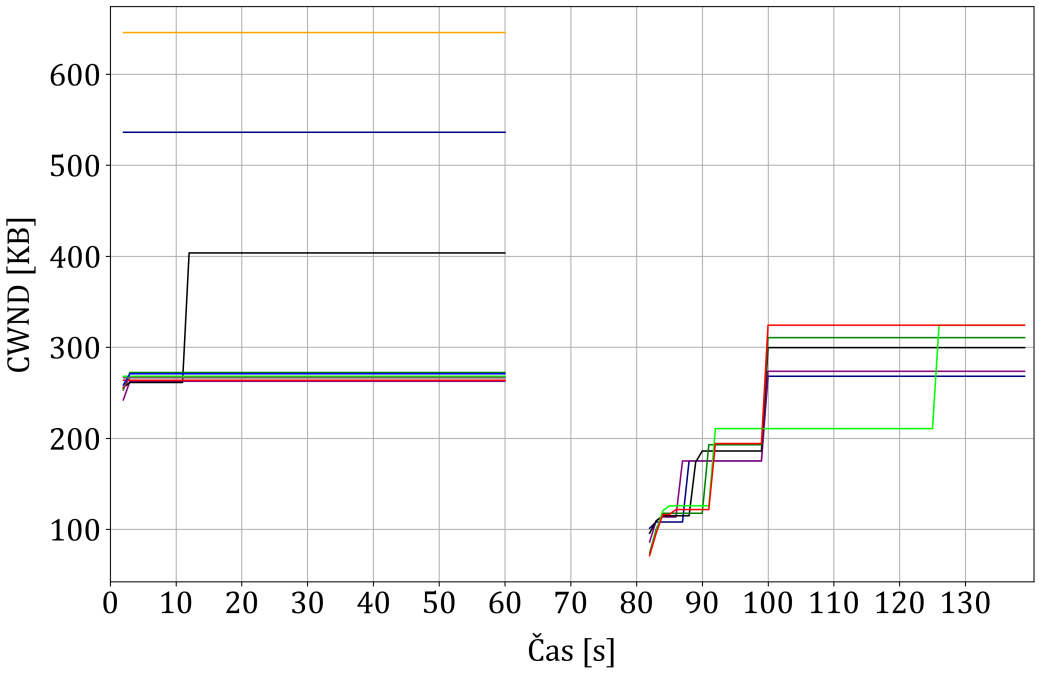
Obrázek B.31: Graf zobrazující naměřenou propustnost sítě scénářem P1 (pohyb z bodu A do bodu C a zpět do bodu A) a Q1.



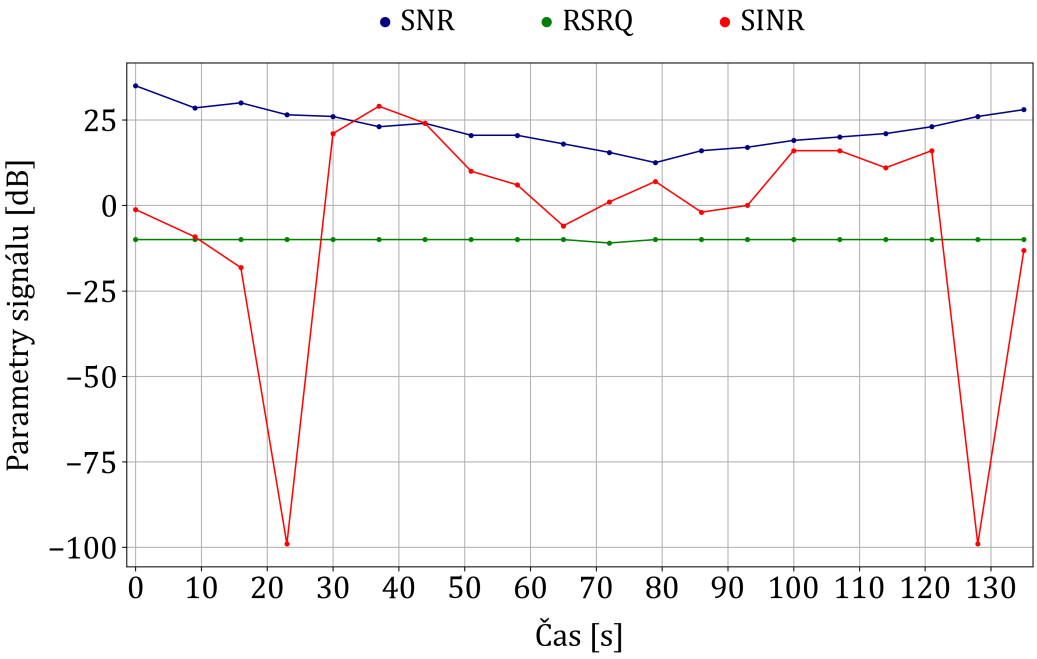
Obrázek B.32: Graf zobrazující naměřené RTT scénářem P1 (pohyb z bodu A do bodu C a zpět do bodu A) a Q1.



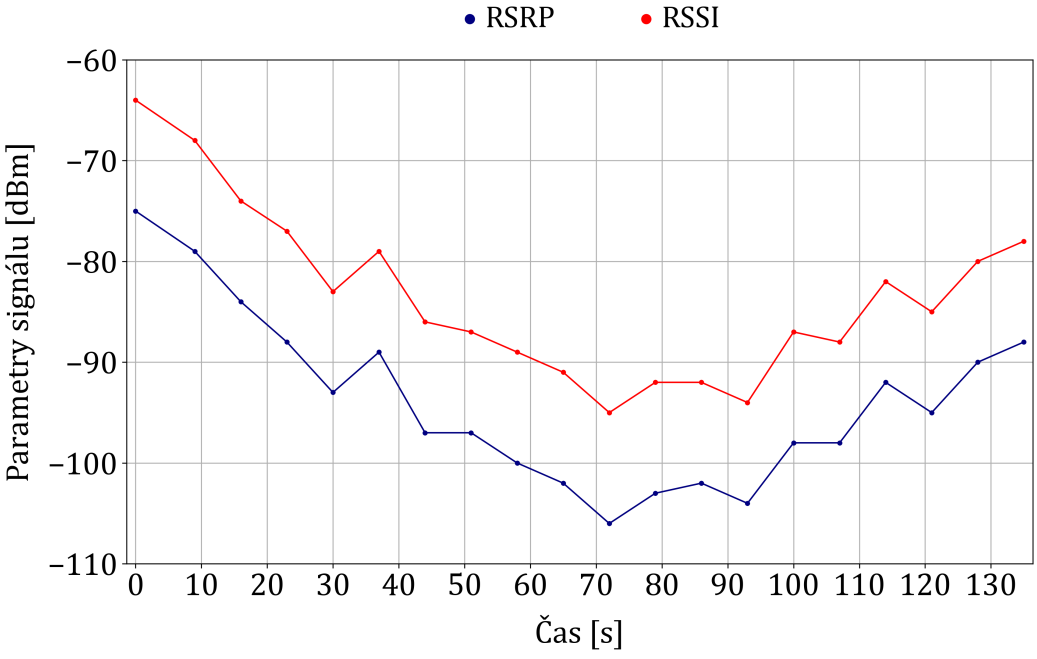
Obrázek B.33: Graf zobrazující rozmezí hodnot RWND během spuštěného scénáře P1 (pohyb z bodu A do bodu C a zpět do bodu A) pro 10 TCP toků (downlink, 0 až 60 s) a 6 TCP toků (uplink, 80 až 140 s).



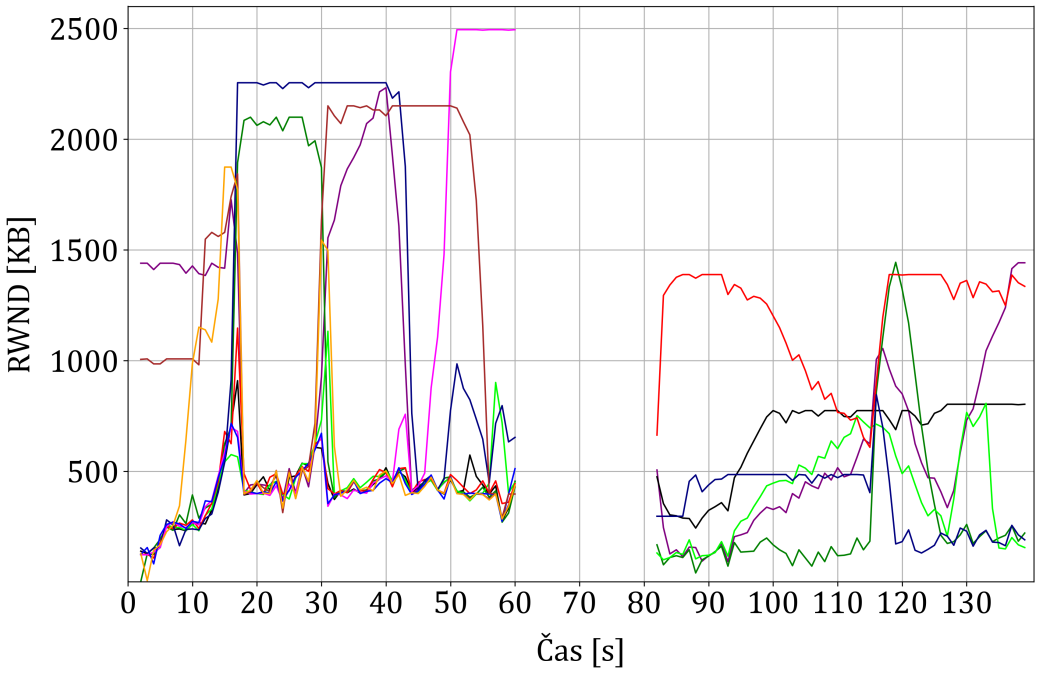
Obrázek B.34: Graf zobrazující rozmezí hodnot CWND během spuštěného scénáře P1 (pohyb z bodu A do bodu C a zpět do bodu A) pro 10 TCP toků (downlink, 0 až 60 s) a 6 TCP toků (uplink, 80 až 140 s).



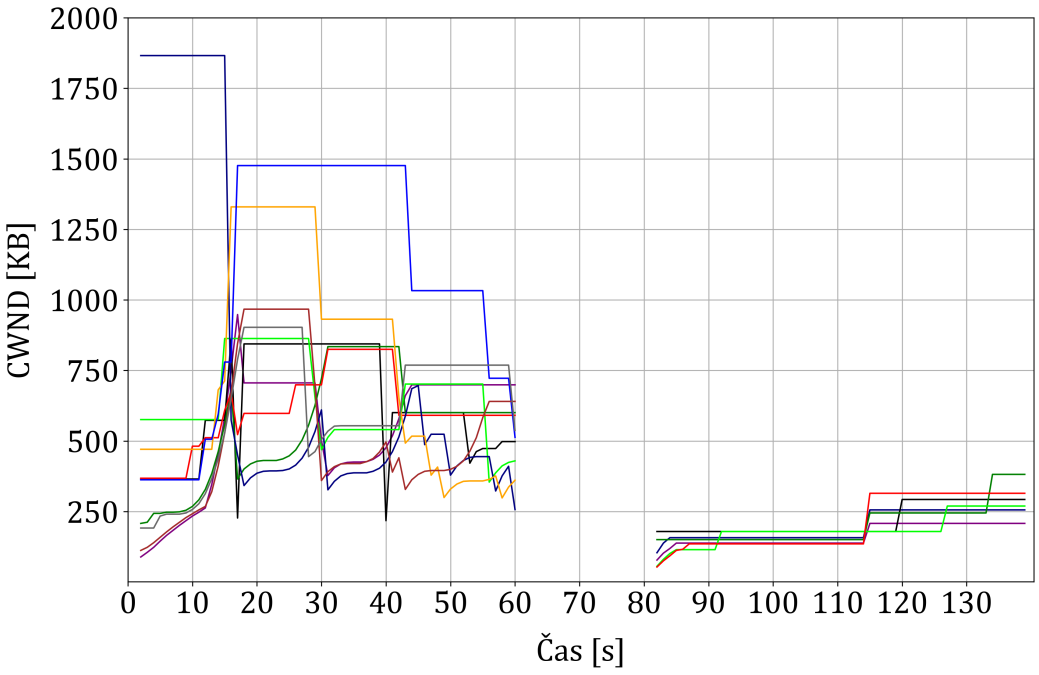
Obrázek B.35: Graf zobrazující naměřené SNR, RSRQ a SINR scénářem P1 (pohyb z bodu A do bodu C a zpět do bodu A).



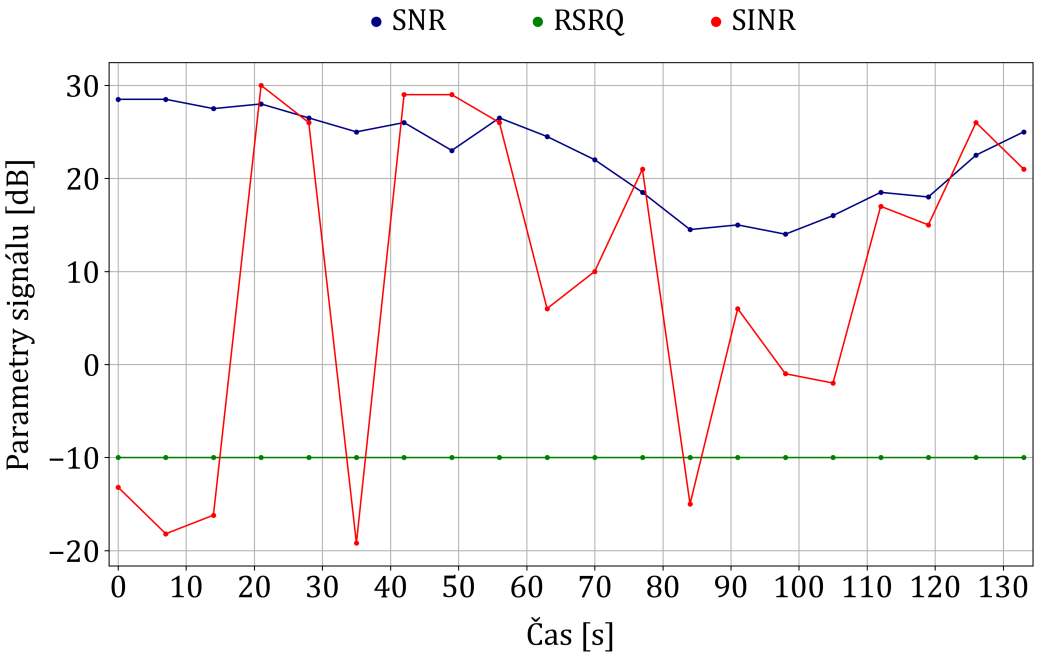
Obrázek B.36: Graf zobrazující naměřené RSRP a RSSI scénářem P1 (pohyb z bodu A do bodu C a zpět do bodu A).



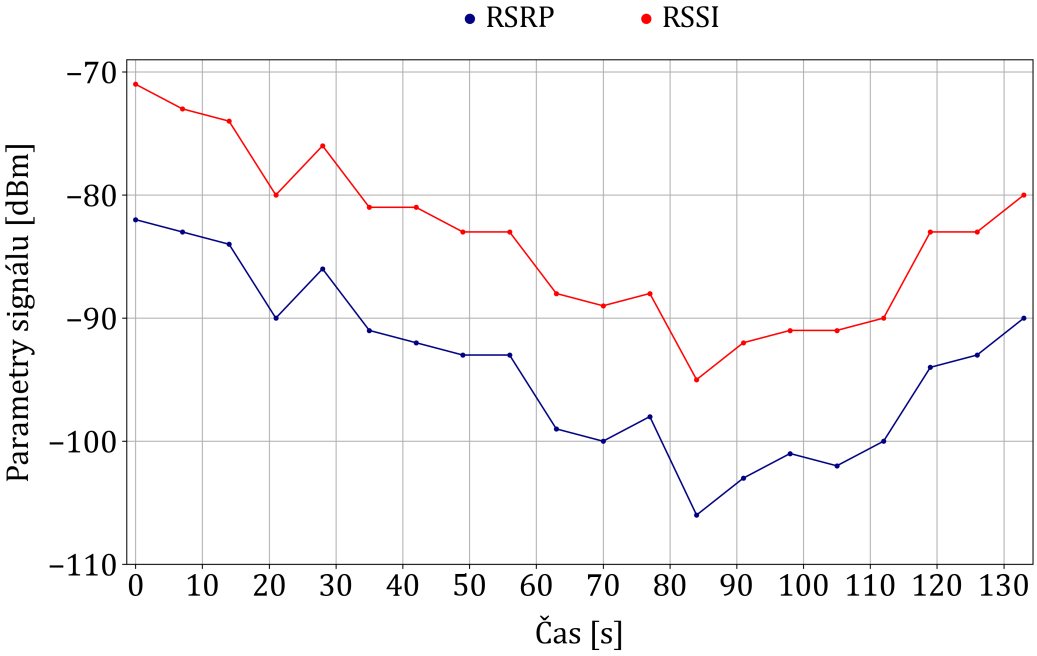
Obrázek B.37: Graf zobrazující rozmezí hodnot RWND během spuštěného scénáře Q1 (pohyb z bodu A do bodu C a zpět do bodu A) pro 10 TCP toků (downlink, 0 až 60 s) a 6 TCP toků (uplink, 80 až 140 s).



Obrázek B.38: Graf zobrazující rozmezí hodnot CWND během spuštěného scénáře Q1 (pohyb z bodu A do bodu C a zpět do bodu A) pro 10 TCP toků (downlink, 0 až 60 s) a 6 TCP toků (uplink, 80 až 140 s).



Obrázek B.39: Graf zobrazující naměřené SNR, RSRQ a SINR scénářem Q1 (pohyb z bodu A do bodu C a zpět do bodu A).



Obrázek B.40: Graf zobrazující naměřené RSRP a RSSI scénářem Q1 (pohyb z bodu A do bodu C a zpět do bodu A).

B.3 Složka obsahující naměřená data

Součástí diplomové práce je složka s naměřenými daty. Složka obsahuje tři podložky `f_tester_5g_fix`, `f_tester_5g_pohyb` a `prvotni_testy`. Jejich obsahem jsou soubory .pdf, .csv a .zip vygenerované platformou F-Tester.