VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIZERTAČNÍ PRÁCE

Brno, 2017 Ing. Tomáš Horváth

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

OPTIMALIZACE SLUŽEB V OPTICKÝCH PŘÍSTUPOVÝCH SÍTÍCH FTTX
SERVICES OPTIMIZATION IN FTTX OPTICAL ACCESS NETWORKS

DIZERTAČNÍ PRÁCE
DOCTORAL THESIS

AUTOR PRÁCE
AUTHOR

Ing. Tomáš Horváth

ŠKOLITEL
SUPERVISOR

prof. Ing. Miloslav Filka, CSc.

BRNO 2017

ABSTRAKT

Tato práce se zabývá optimalizací služeb Triple Play a bezpečností v optických přístupových sítích. První kapitola poskytuje teoretický základ pro vyhodnocení výsledků práce. Druhá kapitola popisuje optické přístupové sítě definované podle ITU. Popsány jsou parametry optických sítí: přenosové rychlosti, dělicí poměr, linkový kód, limitní bitovou chybovost aj. Třetí kapitola vysvětluje současný stav v oblasti budování optických sítí v souladu s plánem rozvoje podle Evropské unie. Praktická část práce je rozdělena do několika podkapitol. Významná část výsledků se věnuje zabezpečení pasivních optických sítí a navržením vhodného zabezpečení pro stávající sítě. K tomuto účelu slouží mimo jiné unikátní parametr doba šíření ve spojení s přepracovaným zabezpečovacím mechanismem. Další podkapitoly se věnují analýze řídicího a datového provozu v gigabitových optických sítích. Výsledky měření byly použitý pro návrh nového algoritmu připojování koncových jednotek, který zkrátí tuto dobu a dále pro návrh algoritmu pro detekci modifikované koncové jednotky. Předposlední podkapitola se zabývá vytvořením ILP modelu pro přenos Triple Play služeb. Poslední podkapitola sestává ze simulací vlastní implementace přenosové vrstvy v simulačním nástroji VPIphotonics.

KLÍČOVÁ SLOVA

pasivní optická síť, bezpečnost, simulace, měření, přenosová vrstva PON, modifikované ONU, ILP

ABSTRACT

This thesis deals with an optimization of Triple play services and security in optical access networks. The first chapter provides theory basics which are necessary for results evaluation. The second chapter describes optical access networks with their parameters such as transmission speed, split ratio, line code, bit error rate etc. defined by ITU. Next chapter summaries the current state in optical networks construction field according to the European Union developing plan. The practical part of this thesis is divided into several subchapters. The significant part of the thesis is dedicated to the security of passive optical networks and design of proper security model for current networks. For this purpose, the unique parameter time propagation T_{prop}, with the novel security model was developed. Next part of the thesis provides an analysis of control traffic and data traffic in the gigabit passive optical networks. For a novel algorithm in activation process in gigabit passive optical networks the measurement results were used. The novel algorithm decreases the total time needed for this process. The last but one subchapter deals with an ILP model for Triple Play services. The last subchapter contains the own implementation of the transmission converge layer in VPIphotonics simulation tool.

KEYWORDS

passive optical network, security, simulation, measurement, transmission convergence layer, rogue ONU, ILP

HORVÁTH, Tomáš *Optimalizace služeb v optických přístupových sítích FTTx*: dizertační práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2017. 137 s. Vedoucí práce byl prof. Ing. Miloslav Filka, CSc.

Vysázeno pomocí balíčku `thesis` verze 2.61; `http://latex.feec.vutbr.cz`

PROHLÁŠENÍ

Prohlašuji, že svou doktorskou práci na téma „Optimalizace služeb v optických přístupových sítích FTTx“ jsem vypracoval(a) samostatně pod vedením vedoucího doktorské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

podpis autora(-ky)

PODĚKOVÁNÍ

V prvé řadě bych rád poděkoval svému školiteli panu prof. Ing. Miloslavu Filkovi, CSc. za odborné rady, konzultaci, trpělivost, ochotu a vedení během mého doktorského studia.
Velký dík patří i sdružení CESNET za technickou podporu během řešení dizertační práce, společnosti Orange SK, jmenovitě Ing. Luboši Dubravcovi, za umožnění měření na jejich síti. Rovněž bych rád poděkoval i svému školiteli ze studijní stáže v Číně, prof. Ning-Hai Bao, Ph.D. za trpělivost během řešení mého ILP modelu a slečně Wen Jin za veškerou pomoc při řešení formalit ohledně stáže.
Nerad bych zapomněl na své kolegy z ústavu Telekomunikací pod vedením prof. Filky. Zejména Ing. Petra Münstera, Ph.D, který je nejen dobrým kolegou, ale i kamarádem. Petrovi vděčím za množství nápadů, inspiraci a mnoho dalšího. Jsem rád, že z mého vedoucího bakalářské práce se stal kolegou a kamarádem zároveň. Stejně tak bych rád vyslovil slova díků i Ing. Ondřeji Havliši za veškerou pomoc, a to nejen v oblasti akademického působení.
Rád bych také poděkoval své přítelkyni Lucii Baierové za trpělivost, kterou se mnou měla během mého doktorského studia a i stále má. Významné poděkování patří i mé rodině, která mě vždy aktivně podporovala již od prvního ročníku studia na vysoké škole.
V neposlední řadě bych rád poděkoval panu Ing. Aleši Buksovi za veškerou podporu, kterou ke mně projevil a za množství motivujících rozhovorů.
I would like to express grateful thanks to my supervisor, prof. Ning-Hai Bao, Ph.D., for his encouragement, patient guidance, and advice during my two internships. You showed me the very interested topics and discussed with me everytime. Thank you very much!

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této doktorské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .

podpis autora(-ky)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

První zmínka o pasivních optických sítích se datuje k roku 1998 (APON). Pilotní standard se úzce opíral o tehdejší technologie, proto byla první pasivní optická síť založená na přenosu ATM buněk. Nebylo možné konstatovat, že by technologie byla masově nasazována pro koncové zákazníky, jako je tomu v dnešní době. Technologie byla nová a velmi průlomová, neboť neobsahovala žádné aktivní prvky podél distribuční sítě. Hlavními zákazníky byly především velké firmy a business zákazníci. S ohledem na daný rok technologie disponovala vysokými přenosovými rychlostmi, a to 155 Mbit/s (pro oba směry) nebo 622 Mbit/s (pro sestupný směr). Nutno však podotknout, že o tuto rychlost se dělili všichni zákazníci připojení k síti.

Další navazující standard byl širokopásmový přístup (BPON). Filosofie a přenosový model zůstal zachován. Významným rozšířením bylo přidání podpory vlnového multiplexu a navýšení přenosových rychlostí na symetrický způsob 622 Mbit/s.

Přestože od prvního zveřejnění samotného přenosového modelu a myšlenky uplynulo již 19 let, nebyla topologie ani myšlenka nijak zásadně pozměněna. Výzkumníci se aktuálně zabývají dalším navýšením přenosových rychlostí v obou směrech. Aktuálně schválená a finalizovaná doporučení podporují přenos 40 Gbit/s v sestupném směru a 10 Gbit/s ve vzestupném směru. Dizertační práce bere v potaz pouze standardy od Mezinárodní telekomunikační unie. V průběhu letitého vývoje se prokázalo, že zachovávání zpětné kompatibility není dlouhodobě únosné z pohledu navyšování přenosových rychlostí a tím i výběru vhodné technologie. Důkazem toho jsou sítě první generace (XG-PON1), které měly za cíl tuto kompatibilitu zachovat, avšak sítě druhé generace (NG-PON2) již tento cíl neměly a dokáží nabídnout 4× vyšší přenosovou rychlost v sestupném směru.

Dizertační práce se zabývá přenosem Triple Play (video, hlas a data) v optických přístupových sítích. Vzhledem k charakteru přenosu informací po optickém vlákně, je nezbytné představit základní myšlenku rychlosti šíření ve vlákně, která je shrnuta v první kapitole spolu s úzce související podkapitolou o detektorech světla. Každá pasivní optická síť je závislá na použitém detektoru a vysvětlení principu je proto nevyhnutelné.

Druhá kapitola poskytuje základní informace o optických přístupových sítích, a to zejména v oblasti vývoje standardů a popisem nejdůležitějších technologií, jak z pohledu budoucího nasazení nejnovějších standardů a jejich vlastností, tak aktuálně dominujících technologií v Evropě. Základní otázkou může být: proč není v současné době nasazována nejnovější technologie a využívá se stále doposud nejpopulárnější technologie po celém světě gigabitové pasivní optické sítě? Zásadním důvodem je cena. Poskytovatelé služeb se na tento fakt zaměřují v každém ohledu. V případě jednoduchého modelu, kde vystačí jedno centrální optické zakončení (OLT),

se bude cena tohoto prvku pohybovat řádově v desetitisících korunách, kdežto počet koncových jednotek může tuto cenu několikanásobně překročit. Bude-li potřeba připojit cca 200 uživatelů a cena koncové jednotky bude 1000 Kč, pak jsou náklady na koncová zařízení 200 000 Kč. V případě nejnovějších standardů jsou ceny koncových jednotek od 7000 Kč výše. Součet položek tvoří pouze základní jednotky, není zahrnuta výstavba sítě, nákup potřebných pasivních prvků aj.

Třetí kapitolu tvoří velice aktuální téma „sítě nové generace v České republice“. Evropská unie se zavázala poskytnout finanční dotaci na pokrytí tzv. „šedých míst“. Tato místa tvoří lokality s velmi omezeným, případně nekvalitním připojením do sítě Internet. Do roku 2020 bude mít každý zákazník k dispozici širokopásmové připojení s minimální rychlostí 30 Mbit/s a nově připojení zákazníci 100 Mbit/s v sestupném směru. Nejvhodnějším kandidátem na dosažení stanovených cílů jsou právě pasivní optické sítě.

Čtvrtou, nejobsáhlejší, kapitolu tvoří praktické výsledky studentské práce. Kapitola je rozdělena do 9 podkapitol, přičemž každá z nich se věnuje specifické oblasti přístupových sítí. První podkapitola pouze teoreticky shrnuje bezpečnostní rizika pasivních optických sítí. Ačkoli je metoda zapouzdření datových rámců, zpravidla Ethernet rámců, do struktury gigabitových sítí dosti složitá, není nemožné ji v reálném čase dekódovat. Dalším příkladem slabin jsou OLT autentizace, správa hesel a kritické řešení modifikované koncové jednotky (ONU), která nerespektuje přidělení časových slotů. Poslední zmíněná problematika je i součástí jednoho doporučení Mezinárodní telekomunikační unie.

Druhá podkapitola se zabývá zvýšením bezpečnosti v gigabitových sítích za využití unikátního parametru, nazývaného parametr šíření. Každá koncová jednotka je v jiné vzdálenosti od řídicí jednotky, a to i v případě, že se nachází na stejném patře v budově. Vždy jsou vytvářeny tzv. rezervy vláken, které vzdálenost prodlužují. Na tuto podkapitolu navazuje další podkapitola, která kompletně mění pohled na zabezpečení gigabitových sítí a prosazuje zcela novou metodu zabezpečení v kombinaci s unikátním parametrem šíření.

Čtvrtá, pátá a šestá podkapitola prezentují simulace aktivačního procesu koncových jednotek, ale také nabízí nový algoritmus pro urychlení tohoto procesu. Současný algoritmus aktivace byl nejen odsimulován, ale také i změřen v síti operátora Orange SK za použití sofistikovaného nástroje GPONxpert. Měřicí přístroj přenášená data (ať už řídicí nebo datové komunikace) přijme, zpracuje a odešle dále do sítě. Dochází tedy k jisté prodlevě a síť je nutno „rozpojit“. Tento úkon může být detekován v řídicím centru operátora. Zachycená data byla použita i pro vyhodnocení a návrh algoritmu detekce modifikované koncové stanice. Šestou podkapitolu tvoří detailní rozbor provozu na síti operátora Orange SK. Zpracováním dat z měřicího přístroje byla nalezena řídicí data, kdy si koncová jednotka stahuje

tzv. konfigurační soubor, průběh komunikace na síti a připojování do multicastového vysílání.

Navazující část je zaměřena na sítě nové generace, jejichž nasazení lze očekávat v průběhu 3–5 let. Vytvořený simulační model měl za cíl poukázat souvislosti s ekvalizačním zpožděním a vzdáleností koncové jednotky. Dostupná doporučení stále vycházejí z tzv. „běžného“ indexu lomu, nicméně index lomu velmi souvisí s vlnovou délkou.

Osmá podkapitola se zaměřuje na vytvoření modelu pasivní optické sítě, nezávislé na použité technologii, za pomocí celočíselného programování. Této oblasti byly věnovány dvě studijní stáže na Chongqing University of Posts and Telecommunications pod vedením prof. Ning-Hai Bao, Ph.D. Výsledný model má za cíl přidělování šířky pásma jednotlivým službám, definovanými požadavky na šířku pásma a prioritou, s ohledem na co nejlepší využití dostupné kapacity linky.

Poslední podkapitolu výsledků studenské práce tvoří implementace přenosové vrstvy pro simulační nástroj VPIphotonics. Veškeré komerčně dostupné nástroje pro simulace optických sítí se zaměřují pouze na fyzickou vrstvu. Implementaci přenosové vrstvy bylo docíleno zabezpečovacího algoritmu, který posouvá limitní bitovou chybovost. Simulační model plně respektuje veškeré parametry fyzické vrstvy a přidává metodu zapouzdření do rámců, jenž jsou přenášený v distribuční části sítě.

1 PŘENOS INFORMACÍ V OPTICKÉM VLÁKNĚ

1.1 Rychlost světla

Dnes, podle dostupných informací, je rychlost světla zcela známá. Nicméně než došlo k úspěšnému odhadu/výpočtu rychlosti světla pokoušela se tuto problematiku osvětlit řada vědců a průkopníků. První snahu o změření rychlosti světla vynaložil italský fyzik Galileo Galilei (1564–1642). Jeho pokus o změření rychlosti světla byl založen na dvou lucernách. Měření probíhalo mezi fyzikem a jeho pomocníkem. Fyzik se svou lucernou byl na jednom kopci a jeho pomocník s druhou lucernou na jiném kopci (vzdálenost mezi kopci byla známa). Poprvé Galileo otevřel (a po krátkém okamžiku ihned zavřel) svou lucernu, a jakmile jeho pomocník spatřil světlo, zopakoval stejné úkony jako fyzik, aby docílil odeslání paprsku na druhou stranu. Po nesčetných pokusech a delších vzdálenostech mezi oběma pozorovateli, Galileo dospěl k závěru, že nejsou schopni (otevřít/zavřít) své lucerny dostatečně rychle, z čehož se domníval, že světlo se šíří nekonečnou rychlostí [1], [2].

Dalším průkopníkem, v oblasti měření rychlosti světla, byl dánský astronom Ole Roemer (1644–1710). Jeho metoda byla založena na pozorování měsíce Io planety Jupiter. K odhadu rychlosti šíření světla využil opakující se jev, zatmění měsíce Io. Samotný astronom si byl dobře vědom toho, že Země obíhá okolo Slunce, čímž je planeta Země jednou Jupiteru blíže a podruhé dále. Rozdíl mezi časy byl $\pm 11\,\text{min}$. Průměrná vzdálenost[1] oběžné dráhy činila $2,901 \cdot 10^{11}\,\text{m}$ [3]. V roce 1676 byla poprvé spočtena rychlost šíření světla c [3]:

$$c = \frac{d}{t} \approx \frac{2,9 \cdot 10^{11} m}{22\,\text{min} \cdot \frac{60 s}{\text{min}}} \approx 2,2 \cdot 10^{8} \frac{m}{s}, \tag{1.1}$$

kde: d je vzdálenost (m), t je čas (s).

V roce 1676 Roamer oznámil, že rychlost světla je $2,25 \cdot 10^{8}\,\text{m/s}$. Jednalo se o historický okamžik, neboť doposud byla rychlost světla brána jako nekonečná.

První úspěšné laboratorní měření rychlosti světla uskutečnil francouzský vědec Arman Fizeau (1819–1896). Základní myšlenka laboratorního měření sestávala z měření celkového času, potřebného k přenosu světla ze zdroje na vzdálené zrcátko a zpět. K měření času Fizeau použil rotující ozubené kolo. Světlo procházející přes jeden „zub“ ozubeného kola je přenášeno na vzdálené zrcadlo a je odraženo zpět. V případě správného nastavení rychlosti otáčení, prochází odražené světlo následujícím „zubem“ v ozubeném kole [4].

[1] Uvažováno v době pokusu.

Na základě tohoto experimentu (v roce 1849) Fizeau spočítal hodnotu rychlosti šíření světla $3,13 \cdot 10^8$ m/s za použití [5]:

$$t = \frac{\theta}{\bar{\omega}}, \tag{1.2}$$

$$c = 2\frac{d}{t}, \tag{1.3}$$

kde: θ je počet rotací (rotace), ω je úhlová rychlost kola (rotace/s), d vzdálenost mezi zdrojem záření a zrcadlem (m), t čas přenosu jedním směrem (s).

K ověření Fizeautovy metody je uvažováno ozubené kolo se 450 zuby a rotační rychlostí 35 otáček/s, zrcátko je ve vzdálenosti 9500 m od ozubeného kola. Pro výpočet rychlosti světla je nezbytné vzdálenost $2d$ vydělit časem Δt, jenž odpovídá času rotace mezi jednotlivými „zuby“ ozubeného kola. Ze známé rychlosti rotace ω kola je možné vypočítat čas za použití vztahu (1.4) [5]:

$$\Delta\theta = \omega\Delta t. \tag{1.4}$$

Potom čas potřebný pro výměnu jednotlivých „zubů“ během rotace je dán [5]:

$$\Delta t = \frac{\Delta\theta}{\omega} = \frac{(1/450rev)}{35rev/s} = 6,3 \cdot 10^{-5}s. \tag{1.5}$$

Výpočet rychlosti šíření světla je dán [5]:

$$c = 2\frac{d}{\Delta t} = \frac{2 \cdot (9500m)}{6,3 \cdot 10^{-5}s} \approx 3 \cdot 10^8 m/s. \tag{1.6}$$

Na práci francouzského vědce dále navazoval jeho pomocník, rovněž francouzský vědec Jean Foucalt (1819–1868), který nahradil v roce 1862 ozubené kolo rotačním zrcátkem. Po zopakování experimentu a následném výpočtu spočítal hodnotu rychlosti šíření světla $2,977 \cdot 10^8$ m/s [4], [5], [6].

Po dobu dalších 60 let byla uvažována hodnota rychlosti šíření světla vycházející z experimentů francouzských vědců. Pokračovatelem zpřesnění hodnoty rychlosti šíření byl americký vědec Albert Abraham Michelson (1852–1931) proslulý svým interferometrem [7]. V roce 1877 vycházel ze stejného principu jako Fizeau a Foucalt, došlo však k nahrazení ozubeného kola malým osmistranným zrcadlem. Je-li rychlost otáčení zrcadla správně nastavena, světlo z jedné strany putuje do pevného zrcadla a může být detekováno po jeho odrazu z jiné strany, která je právě otočena s ohledem na rychlost rotace. Micheslon realizoval svůj experiment mezi Mt. San Antonio a Mt. Wilson v Kalifornii na vzdálenost 35 km. Z výsledku jeho experimentu v roce 1926 vychází hodnota rychlosti šíření světla $c = 2,997 \pm 0,00004 \cdot 10^8$ m/s [8].

Nutno také dodat, že výpis vědců nemusí být kompletní. Dále je nutno poznamenat, že experimentální ověření bylo jednou z možností odhadu/výpočtu rychlosti

šíření světla. V roce 1865 Maxwellova terie popisující elektromagnetické vlnění také umožňovala jednoduché vyjádření rychlosti šíření světla c. Maxwellova teorie o rychlosti šíření elektromagnetických vln ve vakuu je dána [9]:

$$c = \frac{1}{\sqrt{\varepsilon_0 \mu_0}}, \tag{1.7}$$

kde: permitivita vakua $\varepsilon_0 = 8,85 \cdot 10^{-12}$ (C^2/N m^2) a permeabilita vakua $\mu_0 = 4\pi \cdot 10^{-7}$ (T m/A).

Po dosazení c odpovídá:

$$c = \frac{1}{\sqrt{8,85 \cdot 10^{-12} \times 4\pi \cdot 10^{-12}}} = 3 \cdot 10^8 m/s. \tag{1.8}$$

Experimentálně ověřená hodnota a teoretická hodnota si navzájem odpovídají. V současnosti pro přesné výpočty se vychází z hodnoty $c = 299\,796\,458$ m/s, ačkoli pro běžné výpočty dostačuje hodnota z rovnice (1.8).

1.2 Přenos informací po vlákně

Uvažujme jako zdroj signálu CW (Continuous Wave – kontinuální vlna), kontinuální laser, který pracuje na frekvenci ω a je navázán do jednovidového vlákna, pak lze rozložení optického pole popsat ($j = 1$) [10]:

$$\psi(x, y, z, t) = \Phi(x, y, \omega) A(\omega) e^{-i[\omega t - \beta(\omega) z]}. \tag{1.9}$$

Váhový faktor A a rozložení pole v příčném směru Φ se může lišit v závislosti na frekvenci ω. Pro jednoduchost bude dále uvažováno bezztrátové optické vlákno, protože při uvažování ztrát ve vlákně by bylo řešení komplexní, nyní lze propagační konstantu zapsat jako [10]:

$$\beta(\omega) = \beta_r(\omega) + i\alpha(\omega)/2, \tag{1.10}$$

kde: $\beta_r(\omega) = \mathrm{Re}[\beta(\omega)]$ a $\alpha(\omega) = 2\mathrm{Im}[\beta(\omega)]$. Využitím rovnice (1.10) v rovnici (1.9) obdržíme [10]:

$$\psi(x, y, z, t) = \Phi(x, y, \omega) A(\omega) e^{-\alpha(\omega) z/2} e^{-i[\omega t - \beta_r(\omega) z]}. \tag{1.11}$$

Je-li vlákno buzeno několika frekvencemi, celkové rozložení pole je superpozicí polí každé složky [11]:

$$\psi(x, y, z, t) = \Phi(x, y) e^{-\alpha z/2} \sum_{n=1}^{N} A(\omega_n) e^{-i\omega_n t + i\beta_r(\omega_n) z}. \tag{1.12}$$

V rovnici (1.12) je ignorováno rozložení frekvenční závislosti v příčném směru Φ a koeficientu ztrát α. To platí v případě, že frekvence šíření $\Delta\omega = |\omega_N - \omega_1|$ je mnohem menší, než je průměr frekvence dopadajícího pole. V případě, že obálka dopadajícího pole je puls, jeho frekvenční složky jsou těsně u sebe a můžeme nahradit sumu v rovnici (1.12) za integrál [11]:

$$\psi(x, y, z, t) = \Phi(x, y)F(t, z), \tag{1.13}$$

kde:

$$F(t, z) = \frac{e^{-\alpha z/2}}{2\pi} \int_{-\infty}^{\infty} \tilde{A}(\omega) e^{-i[\omega t - \beta_r(\omega) z]} d\omega, \tag{1.14}$$

$$\tilde{A}(\omega) = 2\pi \lim_{\Delta\omega_n \to 0} \frac{A(\omega_n)}{\Delta\omega_n}. \tag{1.15}$$

Z rovnice (1.14) dostaneme [11]:

$$F(t, 0) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \tilde{A}(\omega) e^{-i\omega t} d\omega. \tag{1.16}$$

Rovnice (1.16) reprezentuje Fourierovu transformaci z $\tilde{A}(\omega)$. Proto Fourierova transformace z $\tilde{A}(\omega)$ dopadajícího pulzu $F(t, 0)$ je vyjádřena [11], [12]:

$$\tilde{A}(\omega) = \int_{-\infty}^{+\infty} F(t, 0) e^{i\omega t} dt. \tag{1.17}$$

Tudíž pro daný tvar pulzu lze vypočítat $\tilde{A}(\omega)$ za použití rovnice (1.17) a rozložení optického pole na libovolné z lze vyjádřit z rovnice (1.13) a rovnice (1.14). Následek ve vlákně je charakterizován $\beta(\omega)$. Propagační konstantu na dané frekvenci ω lze vyjádřit na základě propagační konstanty a její odvození na některé frekvenci (zpravidla nosné) ω_0 za použití Taylorovy řady [13], [14]:

$$\beta_r(\omega) = \beta_0 + \beta_1(\omega - \omega_0) + \frac{1}{2}\beta_2(\omega - \omega_0)^2 + \ldots, \tag{1.18}$$

kde:

$$\beta_0 = \beta_r(\omega_0), \tag{1.19}$$

$$\beta_1 = \frac{d\beta_r}{d\omega} |_{\omega=\omega_0} = \frac{1}{v_g}, \tag{1.20}$$

$$\beta_2 = \frac{d^2\beta_r}{d\omega^2} |_{\omega=\omega_0} . \tag{1.21}$$

β_1 je inverzní skupinová rychlost a β_2 je disperzní koeficient druhého řádu. Pokud je šířka pásma signálu mnohem menší než nosná frekvence ω_0, poté lze Taylorovu

řadu zkrátit po druhém členu vpravo. Pro zjednodušení rovnice (1.14) vyberme proměnnou $\Omega = \omega - \omega_0$. Použitím rovnice (1.18) v rovnici (1.14) obdržíme [11]:

$$\begin{aligned} F(t,z) &= \tfrac{1}{2\pi}\textstyle\int_{-\infty}^{+\infty} \tilde{B}(\Omega)\mathrm{e}^{[-\alpha z/2 - i(\omega_0 t - \beta_0 z) + i\beta_1 \Omega z \; + i\beta_2 \Omega^2 z/2]}\mathrm{e}^{(-i\Omega t)d\Omega} \\ &= \tfrac{\mathrm{e}^{[-\alpha z/2 - i(\omega_0 t - \beta_0 z)]}}{2\pi}\textstyle\int_{-\infty}^{+\infty} \tilde{B}(\Omega)\mathrm{e}^{(i\beta_1 \Omega z \; + i\beta_2 \Omega^2 z/2 - i\Omega t)d\Omega} \\ &= \tfrac{\mathrm{e}^{[-i(\omega_0 t - \beta_0 z)]}}{2\pi}\textstyle\int_{-\infty}^{+\infty} \tilde{B}(\Omega) H_f(\Omega, z)\mathrm{e}^{(-i\Omega t)d\Omega}, \end{aligned} \tag{1.22}$$

kde:

$$H_f(\Omega, z) = \mathrm{e}^{(-\alpha z/2 + i\beta_1 \Omega z \; + i\beta_2 \Omega^2 z/2)}, \tag{1.23}$$

je nazývána jako přenosová funkce vlákna a platí [11], [15]:

$$\tilde{B}(\Omega) = \tilde{A}(\omega_0 + \Omega). \tag{1.24}$$

Lineární fázový posun $\beta_1 \Omega z$ odpovídá zpoždění v časové doméně. Uvažujme $\beta_2 = 0$ v rovnici (1.23) a výstup vlákna $z = L$ [11],

$$\begin{aligned} F(t,L) &= \tfrac{\mathrm{e}^{[-\alpha z/2 - i(\omega_0 t - \beta_0 L)]}}{2\pi}\textstyle\int_{-\infty}^{+\infty} \tilde{B}(\Omega)\mathrm{e}^{s[-i\Omega(t - \beta_1 L)]d\Omega} \\ &= \exp[-\alpha z/2 - i(\omega_0 t - \beta_0 L)]B(t - \beta_1 L). \end{aligned} \tag{1.25}$$

V ideálním vlákně (bez disperzí) je $\beta_2 = 0$ pulz, je tedy zpožděn o $\beta_1 L$ na výstupu z vlákna (beze změny jeho tvaru). Použitím rovnice (1.14) v rovnici (1.22), rozložení optického pole je dáno [11]:

$$\psi(x,y,z,t) = \underbrace{\Phi(x,y)}_{\text{příčná osa}} \underbrace{\mathrm{e}^{[-i(\omega_0 t - \beta_0 z)]}}_{\text{nosná}} \underbrace{s(t,z)}_{\text{obálka}}, \tag{1.26}$$

kde:

$$s(t,z) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} \tilde{B}(\Omega) H_f(\Omega, z) e^{(-i\Omega t)d\Omega}, \tag{1.27}$$

$$\tilde{B}(\Omega) = \int_{-\infty}^{+\infty} s(t,0)\mathrm{e}^{(i\Omega t)dt}. \tag{1.28}$$

Rovnici (1.27) s rovnicí (1.28) lze přepsat [11]:

$$s(t,z) = F^{-1}[\tilde{B}(\Omega) H_f(\Omega, z)], \tag{1.29}$$

$$\tilde{B}(\Omega) = F[s(t,0)], \tag{1.30}$$

$$\tilde{B}(\Omega) \rightleftharpoons s(t,0), \tag{1.31}$$

kde: F indikuje Fourierovu transformaci a F^{-1} označuje inverzní Fourierovou transformaci, $\rightleftharpoons$ odpovídá Fourierovým transformovaným párům. Pokud bude uvažováno, že rozložení v příčné ose je shodné na výstupu laseru a na výstupu vlákna, tedy nedojde k žádným změnám podél vlákna, pak pole obálky na výstupu laseru je $s_i(t)$ [11],

$$s_i(t) = s(t,0), \tag{1.32}$$

a

$$\tilde{B}(\Omega) = \mathrm{F}[s_i(t)] = \tilde{s}_i(\Omega). \tag{1.33}$$

Optické vlákno si lze (v tomto případě) představit jako lineární systém s přenosovou funkcí $H_f(\Omega, z)$. Uvažujme, že obálka na výstupu vlákna $s(t,L)$ bude $s_0(t)$ [11],

$$s(t,L) = s_0(t), \tag{1.34}$$

$$F[s_0(t)] = \tilde{s}_0(\Omega) = H_f(\Omega, L)\tilde{s}_i(\Omega). \tag{1.35}$$

Celkové rozložení pole na výstupu je dáno jako [11]:

$$\psi(x,y,L,t) = \Phi(x,y)\mathrm{e}^{[-i(\omega_0 t - \beta_0 L)]s_0(t)}. \tag{1.36}$$

1.3 Detektory světla

V oblasti přístupových sítí jsou zvažovány dva typy fotodetektorů: PIN (Positive-Intrinsic-Negative – fotodioda s velkou neutrálně dopovanou vrstvou mezi p-dopovanými a n-dopovanými oblastmi polovodiče) a APD (Avalanche Photodiode – lavinová dioda). Lavinová dioda nachází své uplatnění zejména pro sítě od 10 Gbit/s a pro zvýšení citlivosti přijímače. Jako zdroj záření pro všechny typy PON sítí je použit laser typu DFB (Distributed FeedBack – laser s rozloženou zpětnou vazbou) [16]. Princip tohoto typu laseru je obecně znám [17], [18], proto jsou v práci popsány pouze výše uvedené typy fotodetektorů.

1.3.1 PIN dioda

PIN dioda nabízí kompromis mezi výkonností a rychlostí. Aktivní oblast je menší, čímž dojde k poklesu doby přechodu a zmenšení optické absorpce (citlivosti). Kvantová efektivita pro osvětlovaný povrch pin diody je dána [19]:

$$\eta = (1 - R) \cdot (1 - e^{-\alpha L}) \tag{1.37}$$

kde: R je odraz povrchu, α je absorpční koeficient a L je aktivní tloušťka vrstvy. Vzhledem k tomu, že absorpční koeficient je funkcí vlnové délky $\alpha = \alpha(\lambda)$, obvykle α klesá se vzrůstající vlnovou délkou λ. Z tohoto důvodu je vlastní odezva vlnově závislá. Limitující šířka pásma doby přechodu světelné absorpce je dána porovnáním doby přechodu pro dva limitní případy $\alpha L \to 0$ a $\alpha L \to \infty$, kde $t_c = t_h = \tau_r$. Doba přechodu frekvenční odezvy pro uniformně osvětlený detektor je dána [19]:

$$|F(\omega)_{\alpha L \to 0}| = \frac{2}{\omega \tau_{tr}} \left[1 + \frac{\sin^2\left(\frac{\omega \tau_{tr}}{2}\right)}{\left(\frac{\omega \tau_{tr}}{2}\right)} - 2\frac{\sin(\omega \tau_{tr})}{(\omega \tau_{tr})} \right]^{1/2}, \tag{1.38}$$

kde: τ_{tr} reprezentuje dobu přechodu.

Pro páry elektrony-díry generované blízko straně p ve vlastní oblasti elektrony přecházejí přes oblast i a frekvenční odezva je dána [20]:

$$|F(\omega)_{\alpha L \to 0}| = \left[\frac{\sin\left(\frac{\omega \tau_{tr}}{2}\right)}{\left(\frac{\omega \tau_{tr}}{2}\right)} \right], \tag{1.39}$$

limitující šířky pásem pro doby přechodu jsou $f_{3dB(\alpha L=0)} = \frac{0{,}45}{\tau_{tr}}$ a $f_{3dB(\alpha L=0)} = \frac{0{,}55}{\tau_{tr}}$ [19], [20], [21]. PIN diody pracující na dlouhých vlnových délkách mají absorpční vrstvy velmi tenkou, proto platí $1 - e^{(-\alpha L)} \approx \alpha L$. Efektivita šířky pásma takového fotodetektoru je dána [19]:

$$\eta \cdot f_{3dB} = 0,45 \alpha v_s, \tag{1.40}$$

kde v_s reprezentuje dobu přechodu elektron-díra.

Z uvedených výpočtů vyplývá, že pokud tloušťka aktivní vrstvy klesá, pak kvantová efektivita pin diody také klesá z důvodu nedostatečné absorpce aktivní vrstvy. Kapacitance klesá s klesající aktivní oblastí. Optimalizace šířky pásma je dosaženo, když limitující doba přechodu je přibližně rovna RC limitní šířce pásma.

Elektrická přenosová funkce se sérií induktancí je dána [20]:

$$H(\omega) = \frac{R_L}{\begin{array}{l}[1 - \omega^2(R_S R_L C_J C_P + L_S(C_J + C_P))] - \\ j\left[\omega(R_L(C_J + C_P) + R_S C_J) - \omega^3 R_S C_J C_P L_S\right]\end{array}}, \tag{1.41}$$

kde: R_L je počáteční resistance, R_S je sériová resistance, C_J je kapacitance spoje, C_P je kapacitance výplně (mezi přichycením polovodiče) a L_S odpovídá sériové induktanci.

Pro dosažení vysoké šířky pásma detektoru je používána dvojitá heterostruktura InP/GaInAS/InP (ve fázi výroby), čímž je docíleno snížení difuzního proudu. Tímto procesem může dojít k omezení impulzní odezvy, která je nyní dána emisní funkcí [20], [21]:

$$e_{e,h}(t) = \frac{1}{\tau_{e,h}} e^{\frac{-t}{\tau_{e,h}}}, \tag{1.42}$$

kde: $e_{e,h}$ je emisní doba pro elektron (díru). Z důvodu zachycení elektronu a díry na druhotném rozhraní je osvětlení pro stranu p dáno [20], [21]:

$$\frac{i_s(\omega)}{i_s(0)} = \frac{1}{(1-e^{-\alpha L})} \left\{ \begin{array}{l} \left(\frac{1-e^{-j\omega t_e}}{j\omega t_e} - e^{-\alpha L}\frac{1-e^{-\alpha L}e^{-j\omega t_e}}{j\omega t_e - \alpha L}\right)\left(\frac{1}{1+j\omega\tau_e}\right) + \\ + \left(\frac{1-e^{-\alpha L}e^{-j\omega t_h}}{j\omega t_e + \alpha L} - e^{-\alpha L}\frac{1-e^{-j\omega t_h}}{j\omega t_h}\right)\left(\frac{1}{1+j\omega\tau_h}\right) \end{array} \right\}, \tag{1.43}$$

a pro stranu n [20], [21]:

$$\frac{i_s(\omega)}{i_s(0)} = \frac{1}{(1-e^{-\alpha L})} \left\{ \begin{array}{l} \left(\frac{1-e^{-\alpha L}e^{-j\omega t_e}}{j\omega t_e + \alpha L} - e^{-\alpha L}\frac{1-e^{-j\omega t_e}}{j\omega t_e}\right)\left(\frac{1}{1+j\omega\tau_e}\right) + \\ + \left(\frac{1-e^{-j\omega t_h}}{j\omega t_h} - e^{-\alpha L}\frac{1-e^{-\alpha L}e^{-j\omega t_h}}{j\omega t_e - \alpha L}\right)\left(\frac{1}{1+j\omega\tau_h}\right) \end{array} \right\}, \tag{1.44}$$

kde: $\tau_{e,h}$ je doba přechodu elektron-díra.

1.3.2 Lavinová dioda

Vysokorychlostní lavinové diody nachází široké uplatnění v optických komunikacích. Lavinové diody s GBP (Gain-Bandwidth Product – součin šířky pásma a k ní příslušejícího zesílení) nad 100 GHz byly představeny v [22], [23] a [24] aj. Pro aplikace pracující na dlouhých vlnových délkách je výhodnější použít lavinové diody InGaAs/InP než Ge diody z důvodu jejich nízkého temného proudu a nižšímu multiplikativnímu šumu. Germániové lavinové diody mají také omezující spektrální odezvu na vlnové délce 1550 nm. V [25] bylo odhadováno, že maximální GBP pro InGaAs/InP dosáhne 140 GHz, kdežto pro Si lavinové diody v oblasti blízké infračervené oblasti může GBP přesáhnout 200 GHz [26]. Vysokorychlostní GaInAS/InP diody využívají oddělené absorpční a násobicí vrstvy.

Pro omezení efektu shromáždění děr je přidáno heterogenní rozhraní mezí absorpční vrstvu a násobicí vrstvu.

Násobicí proces lavinové diody je možné vyjádřit jako koeficient ionizace elektronu a díry α_i a βi. Závislost pole ionizačního koeficientu je dána [27]:

$$\alpha_i(x) = A_e e^{\left(-\frac{B_e}{E(x)}\right)}, \tag{1.45}$$

$$\beta i(x) = A_h e^{\left(-\frac{B_h}{E(x)}\right)}, \tag{1.46}$$

kde: $A_{e,h}$ a $B_{e,h}$ jsou konstantní parametry [27]. Vzhledem k tomu, že elektrické pole je pozičně závislé, ionizační koeficient je rovněž závislý na pozici. Za použití rovnice (1.45) a rovnice (1.46) a rozložení elektrického pole, může být odvozena závislost polohy z ionizačního koeficientu. Nárůst foto proudu v lavinové oblasti ($0 \leq x \leq W$) včetně elektronové proudové hustoty $J_n(0)$, proudové hustoty díry $J_p(0)$ a generace párů elektronů-díry $g(x)$ byl odvozen v [28]. Celková hustota foto proudu je dána [28]:

$$J = \frac{Jp(w)e^{\left[-\int_0^w (\alpha_i - \beta_i)dx\right]} + Jn(0) + q\int_0^w g(x)e^{\left[-\int_0^x (\alpha_i - \beta_i)dx'\right]dx}}{1 - \int_0^w \alpha_i e^{\left[-\int_0^x (\alpha_i - \beta_i)dx'\right]dx}}, \tag{1.47}$$

kde: q je náboj elektronu. Inicializační násobící faktor elektronu (M_n) a díry (M_p) lze vyjádřit při dosazení $J_p(w) = g(x) = 0$ a $J_n(w) = g(x) = 0$ do rovnice (1.47) [28]:

$$M_n = \frac{J}{J_n(0)} = \frac{1}{1 - \int_0^w \alpha_i e^{\left[-\int_0^x (\alpha_i - \beta_i)dx'\right]dx}}, \tag{1.48}$$

$$M_p = \frac{J}{J_p(0)} = \frac{e^{\left[-\int_0^w (\alpha_i - \beta_i)dx\right]}}{1 - \int_0^w \alpha_i e^{\left[-\int_0^x (\alpha_i - \beta_i)dx'\right]dx}}. \tag{1.49}$$

Šířka pásma lavinové diody je limitována RC časovou konstantou, pokud násobící zesílení M je malé ($M < \frac{\alpha_i}{\beta_i}$). Po zvýšení násobícího zesílení nad poměr ionizačního koeficientu elektronu a děr ($M > \frac{\alpha_i}{\beta_i}$). Násobící faktor M jako frekvenční funkci lze následně podle [29] vyjádřit:

$$M(\omega) \approx \frac{Mo}{\sqrt{\{1 + \omega^2 M_o^2 \tau_1^2\}}} \qquad M_o > \frac{\alpha_i}{\beta_i}, \tag{1.50}$$

kde: τ_1 je efektivní čas přechodu, τ je násobicí oblast času přechodu a $N\left(\frac{\alpha_i}{\beta_i}\right)$ reprezentuje počet změn mezi 1/3 a 2 vyjádřených jako $\frac{\alpha_i}{\beta_i}$ lišících se od 1 do 10^{-3}. Stejnosměrný násobící faktor M_o je dán jako [30]:

$$M_o = \frac{1}{1 - \left(\frac{V_j}{V_B}\right)^n}, \tag{1.51}$$

kde: V_j udává přechodné napětí, V_B reprezentuje průrazné napětí a n je empirický faktor ($n < 1$). Celkový temný proud lavinové diody obsahuje dvě složky: I_{du} je

nenásobený proud, který je zejména způsoben únikem proudu z povrchu a I_{dm} je temný proud před zesilovacím procesem, pak je celkový temný proud vyjádřen [20]:

$$I_d = I_{du} + MI_{dm}, \tag{1.52}$$

kde: M je lavinové zesílení. Šum spektrální hustoty proudu vzhledem k temnému proudu je vyjádřen jako [20]:

$$\sigma_d^2 = 2qI_{du} + 2qI_{dm}M^2F(M), \tag{1.53}$$

kde: $F(M)$ je ENF (Excess Noise Factor – statistický šum) [31]. ENF pro inicializační násobící faktor elektronů a děr je vyjádřen [20]:

$$F(M) = F_e(M) = \left[kM + (1-k)\left(2 - \frac{1}{M}\right)\right], \tag{1.54}$$

$$F(M) = F_h(M) = \left[\frac{1}{k}M + \left(1 - \frac{1}{k}\right)\left(2 - \frac{1}{M}\right)\right], \tag{1.55}$$

kde: k je poměr ionizačního koeficientu elektronů a děr $\left(k = \frac{\beta_i}{\alpha_i}\right)$ a k je předpokládaná pozičně nezávislá konstanta. Malá hodnota k znamená menší šumový faktor a tím vyšší citlivost přijímače. Germániové lavinové fotodiody mají k blízké (0,7–1), kdežto GaInAs/InP lavinové diody využívající násobící oblast mají $\frac{1}{k}$ od 0,3 do 0,5. Z pohledu k hodnoty je vynikající materiál pro lavinové diody křemík, neboť jeho k hodnota je 0,02. Pro optické přijímače se používá lavinová dioda s nízkošumovým zesilovačem [32], [33]. Temný proud šumu je dán [20]:

$$\left\langle i_{nd}^2 \right\rangle = 2qI_{du}BI_2 + 2qI_{dm}M^2F(M)BI_2 \tag{1.56}$$

kde: B je bitová rychlost přijímače a I_2 je parametr závislý na vstupním tvaru optického pulzu. Citlivost přijímače lze vyjádřit na základě ε_N [34]:

$$\eta\bar{P} = (1 + \varepsilon_N)\eta\bar{P}_o \tag{1.57}$$

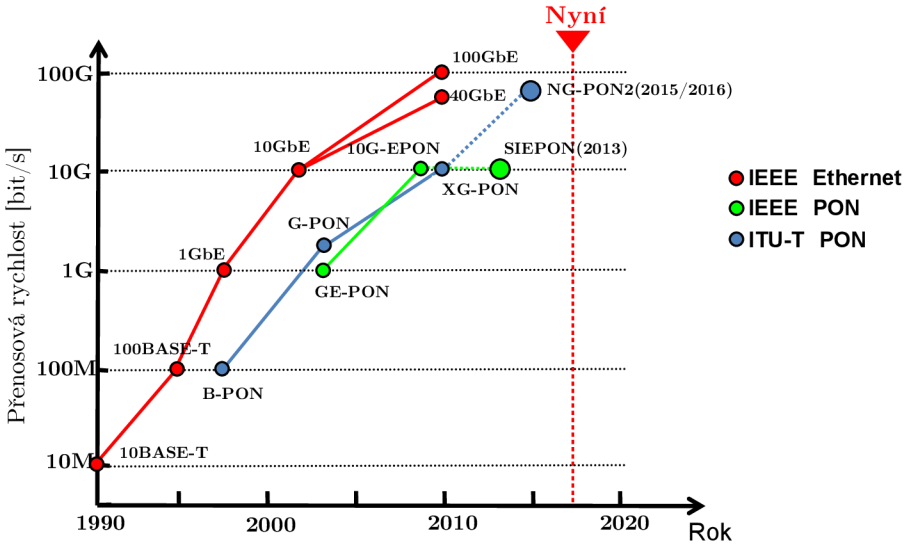
kde: $\eta\bar{P}_o$ je citlivost při nulovém temném proudu. Maximální povolený temný proud pro danou citlivost přijímače je [20]:

$$I_{du} = \frac{\varepsilon_N(2 + \varepsilon_N)}{2qBI_2}\left\langle i_{na}^2 \right\rangle \tag{1.58}$$

kde: $\langle i_{na}^2 \rangle$ je zesílení výkonu šumu a je přímo úměrné B nad 100 Mbit/s.

2 OPTICKÉ PŘÍSTUPOVÉ SÍTĚ

V současné době jsou pasivní optické sítě považovány za sítě budoucnosti. Jejich světová rozšířenost je dána geografickou polohou. Pro přístupové sítě v Evropě nyní dominuje standard podle ITU (International Telecommunication Union – Mezinárodní telekomunikační unie), kdežto přístupové sítě v Asii pracovaly se standardy podle doporučení IEEE (Institute of Electrical and Electronics Engineers – institut pro elektrotechnické a elektronické inženýrství). Dosavadní vývoj standardů pro pasivní optické sítě zobrazuje obr. 2.1. Z obr. 2.1 je patrný náskok Mezinárodní telekomunikační unie ve vývoji standardů pro optické přístupové sítě. Na druhou stranu, oblíbenost konkurenčních doporučení v asijských zemích byla dána jejich snadnou implementací, neboť datové jednotky jsou přenášeny ve formě ethernetovského rámce, čímž je usnadněna správa těchto sítí. Doporučeními IEEE se tato práce nezabývá, neboť tato problematika byla hojně publikována jak na světových konferencích, tak v uznávaných časopisech.



Obr. 2.1: Dosavadní vývoj standardů pasivních optických sítí [35]

2.1 GPON

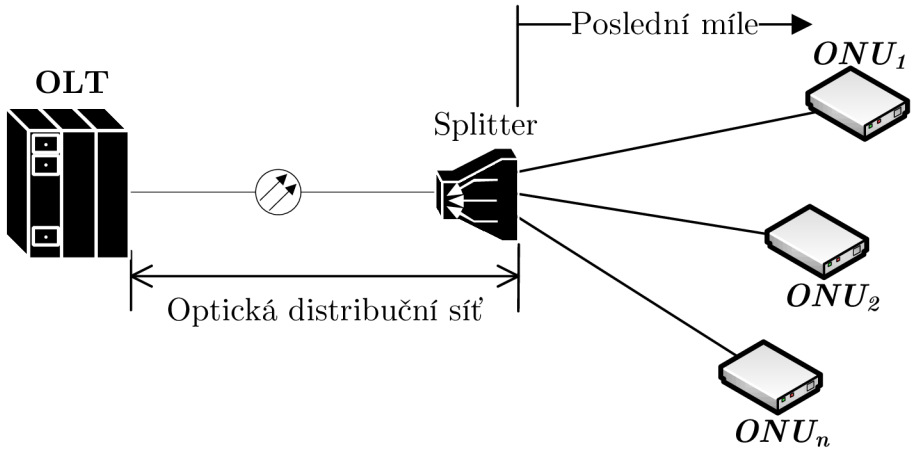
Tato podkapitola pojednává o nejrozšířenějším standardu pasivních optických sítí v Evropě. Prvotní představení standardu GPON (Gigabit Passive Optical Network – gigabitová pasivní optická síť) proběhlo v roce 2003. Jednalo se o prvotní model gigabitové přípojky, kterou lze použít v domácnostech k připojení Triple Play (video, hlas a data) služeb. Zásadním rozdílem mezi předchozími doporučeními byla již

zmíněná přenosová rychlost, podpora přenosu Ethernetu po optické síti (ten však je zcela nezbytné zapouzdřit do rámce, jenž je přenášen v těchto sítích), zvýšení dělicího poměru (na jeden segment sítě bylo možno připojit až 128 koncových zákazníků), stanovení útlumových tříd, nadefinování výkonových úrovní aj.

Klíčové vlastnosti tohoto standardu mohou být shrnuty následovně [36]:

- přenosová rychlost – sestupný směr – 1,25; 2,45 Gbit/s,
- přenosová rychlost – vzestupný směr – 0,155; 0,622; 1,24; 2,48 Gbit/s,
- maximální délka distribuční sítě 20 km, 40–60 km pro sítě s prodlouženým dosahem,
- maximální dělicí poměr v distribuční síti 1:128,
- NRZ (Non Return Zero – linkový kód bez návratu k nule) linkový kód pro přenos informací,
- útlumový rozsah pro distribuční síť 5–35 dB,
- kritická bitová chybovost pro přenos 10^{-10} bez korekčního kódu, 10^{-4} s FEC (Forward Error Correction – dopředná korekce chyb).

Dosavadní výzkum pasivní optické sítě GPON pokrývá výhradně fyzickou vrstvu nebo koexistenci s novějšími standardy [37], [38], [39]. Její klíčové vlastnosti byly popsány výše. Architekturu pasivních optických sítí lze shrnout pomocí obr. 2.2.



Obr. 2.2: Architektura GPON sítě

Z obr. 2.2 je patrná přítomnost jak řídicí jednotky, tak koncové jednotky. Řídicí jednotka OLT (Optical Line Termination – optické linkové zakončení) bývá umístěna zpravidla v části, kterou spravuje (nebo má k ní přístup) ISP (Internet Service Provider – poskytovatel připojení k Internetu), tedy poskytovatel služeb. Koncová jednotka ONU (Optical Network Unit – optická síťová jednotka) ukončuje optickou část sítě a provádí konverzi optického signálu na elektrický, zpravidla optoelektronickým převodníkem s PIN nebo APD diodou.

2.2 X(N)G-PON

Další milník pro vývoj standardů pasivních optických sítí tvoří projekt N(X)G-PON (Next Generation PON – pasivní optická síť další generace). Projekt byl tvořen dvěma fázemi, neboť bylo nezbytné se zabývat dalším vývojem z hlediska:

- zachování zpětné kompatibility,
- nalezení jiné vhodné technologie, kterou by šlo považovat za nástupce doposud využívané WDM (Wavelength Division Multiplexing – vlnově dělený multiplex) technologie, tedy vlnového dělení.

Výsledkem první etapy bylo doporučení ITU-T G.987, označováno jako XG-PON. Předchozí (GPON) i nově navržený (XG-PON) standard pracuje na rozdílných vlnových délkách, přesto je zachována zpětná kompatibilita i koexistence. Doporučení [40] specifikuje dvě možnosti koexistence: v rámci jedné sítě nebo pomocí koexistenčního členu, čímž je docíleno sdílení ODN (Optical Distribution Network – optická distribuční síť).

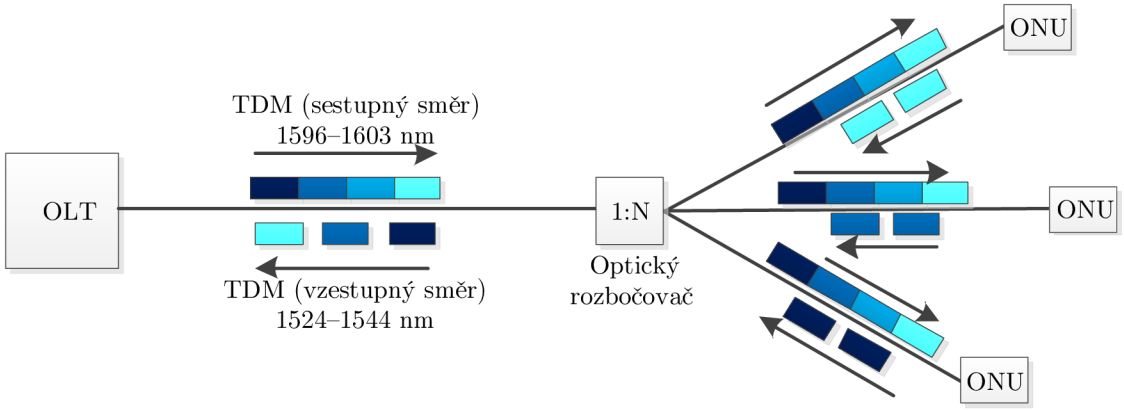
Klíčové vlastnosti výsledku první etapy projektu NG-PON lze shrnout následovně [40]:

- přenosová rychlost – sestupný směr – 2,48; 9,95 Gbit/s,
- přenosová rychlost – vzestupný směr – 2,48; 9,95 Gbit/s,
- maximální délka distribuční sítě 20 km, 40–60 km pro sítě s prodlouženým dosahem,
- maximální dělicí poměr v distribuční síti minimálně 1:128 (volitelně až 1:256),
- NRZ linkový kód pro přenos informací,
- útlumový rozsah pro distribuční síť 14–35 dB,
- kritická bitová chybovost pro přenos 10^{-10} bez korekčního kódu, 10^{-4} s protichybovým zabezpečením FEC.

2.3 NG-PON2

Předešlá podkapitola se zabývala výsledkem první fáze projektu NG-PON. Světoví výrobci (Huawei, Alcatel Lucent aj.) se naopak podílejí na vývoji druhé etapy, která nemá za povinnost zachovat zpětnou kompatibilitu s dřívějšími standardy. Autoři [41] se zabývali, která z etap bude ve finále označována za „vítěze“, neboť výsledek první etapy umožní využít stávající komunikační jednotky, kdežto NG-PON2 (Next Generation PON Stage 2 – pasivní optická síť druhé generace) standard vyžaduje přeladitelné filtry na straně zákazníka. V současné době vznikla první verze doporučení ITU-T G.989. Před jeho samotným schválením docházelo

k výběru vhodné technologie, kterou bude tento standard využívat [42]. Výsledkem dohody mezi ITU a světovými operátory byla technologie TWDM-PON (Time Wavelength Division Multiplexing PON – pasivní optická síť na principu časového a vlnového multiplexu). Obecný princip TDM (Time Division Multiplex – časově dělený multiplex) technologie zobrazuje obr. 2.3. Otázkou zůstává, kterou z etap si zvolí operátoři k vybudování nové sítě. Nutná investice ze strany poskytovatele služeb bude tedy zásadní, jestliže operátor doposud nevlastní síť, bude probíhat výstavba sítě podle [43] na tzn. „zelené louce“. Při tomto scénáři je pro ISP vhodné zvážit počáteční vyšší investici do prvků, které pracují na standardu NG-PON2 [44].



Obr. 2.3: Princip TDM technologie pro sítě NG-PON2

Jedná se především o použitý typ vlákna v distribuční síti, minimální dělicí poměr, předpokládané linkové kódy atd. Klíčové vlastnosti standardu NG-PON2 lze shrnout následovně [45]:

- přenosová rychlost – sestupný směr – 10; 40 Gbit/s (v závislosti na použitém počtu páru vlnových délek),
- přenosová rychlost – vzestupný směr – 10; 40 Gbit/s,
- maximální délka distribuční sítě 20–40 km, 40–60 km pro sítě s prodlouženým dosahem,
- maximální dělicí poměr v distribuční síti minimálně 1:256 (předpokládá se 1:512),
- NRZ a Millerův linkový kód (doporučení [45] kód pouze uvádí, neuvádí jej pro nasazení) pro přenos informací,
- útlumový rozsah pro distribuční síť 14–35 dB,
- kritická bitová chybovost pro přenos 10^{-10} bez korekčního kódu, 10^{-4} s protichybovým zabezpečením FEC.

Porovnání všech doposud popsaných standardů poskytuje tab. 2.1 a tab. 2.2.

Tab. 2.1: Porovnání vlastností GPON, XG-PON a NG-PON2 sítí pro sestupný směr.

	GPON	XG-PON	NG-PON2
Rychlost [Gbit/s]	2,45	9,95	40
Použité vlákno	G.652	G.652	G.652
Dosah systému [km]	20	20	20–40
Linkový kód	NRZ	NRZ	NRZ, Miller
λ [nm]	1480–1500	1575–1580	1596–1603
Počet párů λ	—	—	1–4
BER	10^{-10}	10^{-10}	10^{-12}

Tab. 2.2: Porovnání vlastností GPON, XG-PON a NG-PON2 sítí pro vzestupný směr.

	GPON	XG-PON	NG-PON2
Rychlost [Gbit/s]	1,25	2,48	10
Použité vlákno	G.652	G.652	G.652
Dosah systému [km]	20	20	20–40
Linkový kód	NRZ	NRZ	NRZ, Miller
λ [nm]	1260–1360	1260–1280	1524–1544
Počet párů λ	—	—	1–4
BER	10^{-10}	10^{-10}	10^{-12}

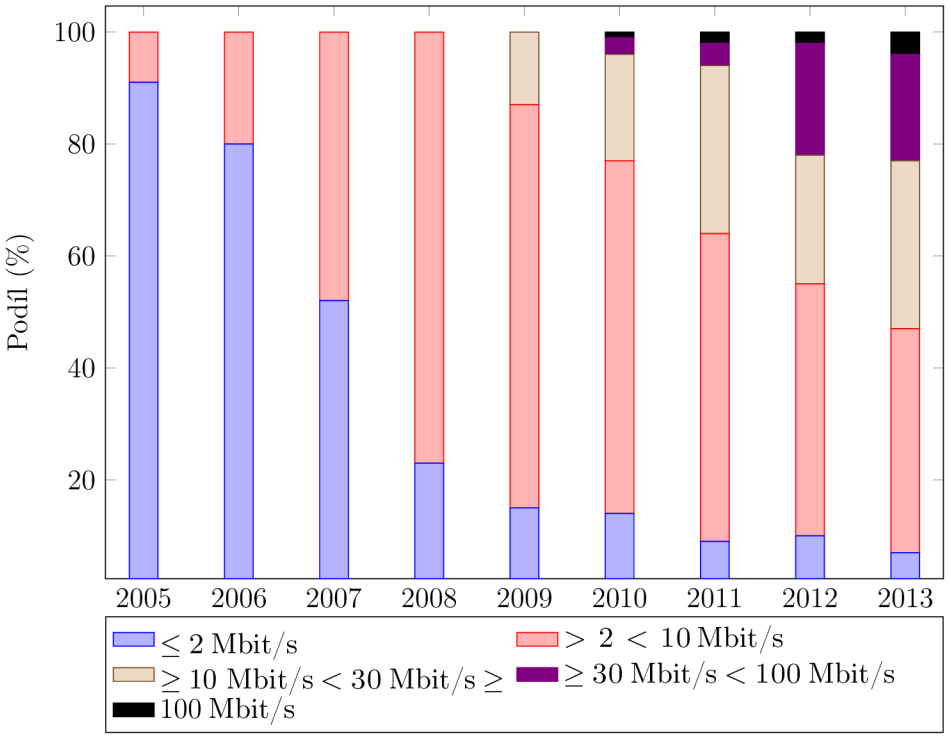
3 SÍTĚ NOVÉ GENERACE V ČESKÉ REPUBLICE

Česká republika se v rámci Evropské unie zavázala, že zajistí přenosovou rychlost alespoň 30 Mbit/s ve směru k uživateli do roku 2018 [46], dalším milníkem pak bude rok 2020, kde rychlost v sestupném směru má dosáhnout 100 Mbit/s pro polovinu domácností [46]. Obě uvedené varianty počítají s nesymetrickými přenosovými rychlostmi, tedy zpravidla vyšší rychlostí pro sestupný směr. Tento „nedostatek“ by měl být eliminován do roku 2030, neboť v tomto roce, na základě [47], je uvažována pouze symetrická varianta přístupu k Internetu.

Takovéto nároky na přenosovou rychlost již nedokáží splnit veškeré technologie např. ADSL (Asymmetric Digital Subscriber Line – asymetrická digitální linka). V plánech České republiky se hojně zmiňuje pasivní optická síť typu GPON, nebo varianty aktivní optické sítě. Formální definici pro sítě nové generace lze na základě [48] definovat takto: NGN (Next Generation Networks – sítě nové generace) jsou sítě založené na technice přenosu datových paketů, které jsou schopné zajišťovat služby elektronických komunikací s tím, že umožňují využívat rozličné vysokorychlostní přenosové technologie schopné řídit a kontrolovat kvalitu poskytovaných služeb a jejichž funkce vztažené k poskytovaným službám jsou nezávislé na základních přenosových technologiích. Síť poskytuje účastníkům neomezený přístup k různým poskytovatelům veřejně dostupných služeb elektronických komunikací a důsledně podporuje poskytování služeb účastníkům v kterémkoliv místě sítě. Rovněž sítě nové generace lze rozdělit na páteřní a přístupové. Tato práce se věnuje výhradně přístupovým sítím.

Na druhou stranu Česká republika není zcela připravena uspokojit vysoké nároky na rychlost připojení ve všech lokalitách. Na základě [49] vyplývá, že dominující přenosové rychlosti byly do 10 Mbit/s (viz obr. 3.1). Vyšší přenosové rychlosti nezaznamenávají významný růst.

V roce 2016 publikoval Český telekomunikační úřad výroční zprávu, kde je souhrn aktuálních technologií pro přístup k Internetu. Graf je zobrazen na obr. 3.2. Na základě obr. 3.2 je patrné, že dominující technologií je WiFi (26,8 %), tedy bezdrátový přenos informací. Výroční zpráva neuvádí použité frekvence, lze však předpokládat základní kmitočty v bezlicenčním pásmu (2,5/5 GHz). Druhou technologií s nejvyšší penetrací pokrývají mobilní sítě se zastoupením 23,2 %. Třetí technologie sdružuje veškeré typy xDSL připojení, kde dominující postavení na trhu má společnost Telefónica O2 Czech Republic, a. s., jenž disponuje penetraci 20,6 %, pouhých 3,5 % připadá jiným provozovatelům xDSL připojení. V návaznosti na [47] jsou FTTx (Fiber to the ... – optické vlákno do ...) přípojky na shodné hodnotě penetrace



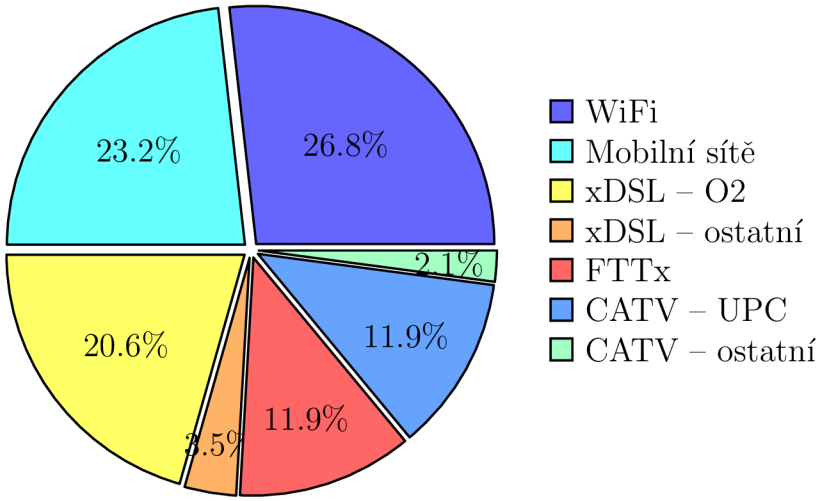
Obr. 3.1: Vývoj přenosových rychlostí podle [49]

(11,9 %) se společností UPC Česká republika, s. r. o. Kabelový operátor UPC Česká republika, s. r. o. v současnosti nabízí nejvyšší rychlost připojení 400/40 Mbit/s v závislosti na lokalitě. Naopak přípojky FTTx jsou závislé pouze na zvoleném standardu a mohou podporovat při FTTH (Fiber to the Home – optické vlákno do bytu) variantě přenosovou rychlost až 10/10 Gbit/s[1] (sdíleně v závislosti na počtu koncových jednotek připojených k řídicí jednotce OLT).

Obecně se rozlišují nejznámější FTTx přípojky:

- FTTN (Fiber to the Node – optické vlákno do distribučního uzlu) – jedná se o metodu zakončení optického vlákna, které je přivedeno do distribučního uzlu a od něj je dále rozváděn signál již pomocí metalických rozvodů ke všem koncovým uživatelům.
- FTTC (Fiber to the Curb – optické vlákno k obrubníku) – optické vlákno je přivedeno do účastnického rozvaděče (zpravidla na velkém sídlišti), od kterého vedou metalické rozvody ke koncovým zákazníkům.
- FTTB (Fiber to the Building – optické vlákno do budovy) – optické vlákno je přivedeno až k budově, ve které sídlí koncoví zákazníci. Vlákno je zakončeno zpravidla ve sklepení této budovy a dále je signál ke koncovým zákazníkům

[1] Při úvaze standardu dle [40].



Obr. 3.2: Technologie pro přístup k Internetu v ČR na základě [50]

rozveden pomocí metalických spojů. V praxi se vyskytují i varianty, kdy jsou budovy propojeny vzájemně například bezdrátovým vysokorychlostním spojem.

- FTTH (Fiber to the Home – optické vlákno do bytu) – koncovými zákazníky nejvíce oblíbená metoda zakončení optického vlákna. Koncovým zákazníkům je optické vlákno přivedeno až do jejich bytu. Tento způsob zakončení umožňuje nasazení nejvyšších přenosových rychlostí od/k zákazníkovi. Dnešní připojení k Internetu od společnosti Google využívá právě tuto metodu.
- FTTO (Fiber to the Office – optické vlákno do kanceláře) – optické vlákno je přivedeno do kanceláře zákazníka. Cílem není nabídnout nejvyšší rychlost do kanceláře, nýbrž zajistit kvalitní a stálé připojení k Internetu s garantovanými parametry, které jsou se společnosti sjednány.
- FTTA (Fiber to the Antenna – optické vlákno k anténě) – v poslední době velice oblíbený styl zakončení optického vlákna ve vysílači rádiového signálu pokrývající danou oblast mobilním signálem.

Vlastnosti přístupových sítí nové generace podle [51] lze shrnout následovně:

- zajištění vysoké přenosové rychlosti pro účastníka/ky a poskytovat spolehlivé služby, a to pomocí sítě z optických vláken nebo jiné srovnatelné technologie,
- rozmanitá podpora vyspělých digitálních a konvergovaných služeb na technologii IP (Internet Protocol – internetový protokol),
- poskytování podstatně vyšší přenosové rychlosti v sestupném směru, tedy ve směru k uživateli.

V současnosti se za odpovídající přístupové sítě nové generace považují [51]:

- přístupové sítě založené na optických vláknech,
- adekvátně modernizovaná kabelová síť,
- některé bezdrátové přístupové sítě, přes které lze nabídnout spolehlivé vysokorychlostní[2] připojení.

[2]Vysokorychlostním připojení se rozumí minimálně 30 Mbit/s ve směru k účastníkovi [51].

CÍLE DIZERTAČNÍ PRÁCE

Sítě podle FTTx nacházejí stále větší oblibu jako vhodná metoda pro připojení budoucích klientů. Poskytovatelé služeb vybudují distribuční část sítě, kterou je možné využít i pro novější technologie pasivních optických sítí. Jednoduchým nahrazením řídicí jednotky a koncových jednotek mohou nabídnout vyšší tarify pro své zákazníky. Optické přenosy jsou obecně považovány za bezpečné, nicméně je dispozici řada bezpečnostních rizik těchto sítí. Metoda zapouzdření dat značně znesnadňuje případné odposlechy. Významnou roli hraje aktivační proces ONU, který udává za jakou dobu bude veškerá komunikace obnovena pro všechny zákazníky. Současné simulační nástroje podporují simulace pouze fyzické vrstvy s vyhodnocením bitové chybovosti nebo diagramu oka. Pro bližší prozkoumání problematiky pasivních optických sítí byly navrženy následující hlavní cíle dizertační práce:

- Rozbor aktuální penetrace technologií pro připojení k Internetu.
- Vyhodnocení základních bezpečnostních rizik pasivních optických sítí:
  - prozkoumání problematiky distribuce klíče k zabezpečení komunikace mezi jednotkou OLT a ONU,
  - zvýšení bezpečnosti gigabitových sítí unikátním parametrem,
  - optimalizace stávajícího řešení distribuce klíče mezi OLT a ONU,
  - návrh robustního modelu pro zabezpečení gigabitových sítí.
- Vytvoření simulace, na základě reálných náměrů, aktivačního procesu a navržení optimalizace za účelem snížení doby připojení všech koncových jednotek:
  - analýza průběhu spojení mezi jednotkami OLT a ONU během prvotní inicializace spojení,
  - zaměření se na problémy vysokých dělicích poměrů z pohledu doby připojení koncových jednotek,
  - optimalizace průběhu navázání spojení mezi jednotkami a zkrácení doby pro ustanovení spojení.
- Navržení detekčního algoritmu pro lokaci modifikované koncové jednotky, která nerespektuje přidělené časové sloty.
- Analýza datové komunikace v gigabitových pasivních optických sítích pro oba směry.
- Posouzení vlivu ekvalizačního zpoždění na čas připojení během aktivačního procesu pro sítě nové generace.
- Vytvoření obecného matematického popisu pasivních optických sítí pomocí celočíselného programování.
- Implementace přenosové vrstvy do simulačního nástroje VPIphotonics.
  - tvorba simulace s/bez přenosové vrstvy s posouzením vlivu na celkový dosah systému.

4 VÝSLEDKY STUDENTSKÉ PRÁCE

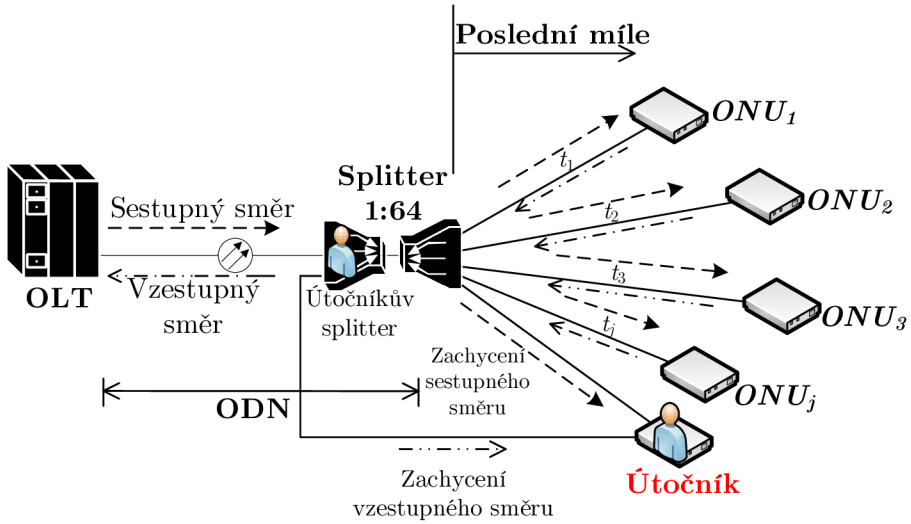
4.1 Bezpečnostní rizika GPON sítí

Pasivní optické sítě nacházejí stále větší uplatnění v přístupových sítích. Jejich hlavní dominantou je kompletně pasivní infrastruktura, tedy poskytovatel služeb se nemusí zabývat problematikou zajištění elektrické energie pro aktivní prvky. Na druhou stranu tuto výhodu lze považovat i jako nevýhodu, a to z důvodu omezení šířky pásma pro koncové účastníky (aktivní sítě zpravidla nabízejí „neomezenu“ šířku pásma).

4.1.1 Zabezpečení datové komunikace

Obecně PON sítě jsou realizovány na principu P2MP (Point to Multipoint – spojení bod-mnohobod) spojení, tedy od jednoho zdroje se datová jednotka[1] šíří k více příjemcům. Jinými slovy lze tuto topologii chápat jako komunikaci master-slave, kde OLT jednotka vystupuje v roli master a veškeré koncové jednotky ONU jsou v roli slave. Řídicí jednotka OLT spravuje veškerou komunikaci (do obou směrů), časové sloty a dynamické přidělování šířky pásma. Z principu chování PON není možné odeslat data jediné koncové jednotce. Každý rámec je odeslán všem koncovým jednotkám, avšak zpracován je pouze v koncové jednotce s odpovídajícími parametry, ostatní ONU rámce zahazují. Z pohledu útočníka je možné naslouchat oba směry, nicméně sestupný směr pro odposlech je konstrukčně méně náročný, protože nevyžaduje změnu v topologii. Poskytovatelé služeb zpravidla neuvažují modelové případy jednotlivých doporučení (jeden splitter s vysokým dělicím poměrem), ale používá se kaskádního zapojení rozbočovačů. Poslední splittery jsou umístěny v neobytných prostorech budov (sklepních prostorech) a dále jsou vedena jiná optická vlákna do bytu/přípojky zákazníka. Připojením koncové jednotky (ve většině případů s modifikovaným firmwarem) do volného portu rozbočovače, může útočník naslouchat veškerou komunikaci v sestupném směru. Odposlech vzestupného směru je technicky náročnější, neboť je vyžadováno fyzické odpojení splitteru pro připojení dalšího splitteru. Zapříčiněný výpad spojení povede k rozpadu synchronizace mezi OLT a ONU jednotkami na daném splitteru a zvýšení vložného útlumu v trase (poskytovatel služeb je schopen detekovat změnu topologie). Princip připojení pro oba směry je zobrazen na obr. 4.1. Dalším ohrožujícím faktorem je známá struktura

[1] V GPON sítích se jedná o GTC (Gigabit Passive Optical Network Transmission Convergence – přenosová vrstva GPON sítí) rámce, které obsahují GEM (Gigabit-capable passive optical network Encapsulation Method – zapouzdřovací metoda pro GPON sítě) rámce nesoucí důležitá pole pro komunikaci.

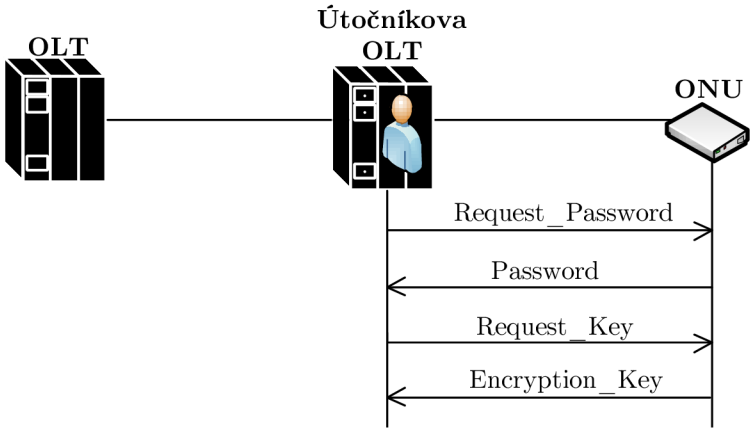


Obr. 4.1: Odposlech sestupného a vzestupného směru v GPON síti

jak GTC, tak GEM rámců pro GPON sítě, definováno v [53]. Analýza v reálném čase je možná při použití FPGA (Field-Programmable Gate Array – programovatelná hradlová pole) [54]. Z výše uvedených faktorů vyplývá nezbytnost zabezpečení datové komunikace. V reálných sítích je zabezpečení komunikace pouze volitelnou položkou, která je ve výchozí konfiguraci vypnutá [52].

4.1.2 OLT autentizace

Druhým bezpečnostním aspektem lze uvažovat samotnou autentizaci. V průběhu aktivačního procesu ONU jednotky, OLT autentizuje každou ONU jednotku, ale opačná autentizace zcela chybí. Proto lze uvažovat, že útočník může podvrhnout svou OLT jednotku pro vzestupný směr. Připojení OLT jednotky útočníka by se neobešlo bez výpadku spojení. Tento výpadek by poskytovatel služeb zaznamenal (například alarmem v dohledovém centru), nicméně po připojení falešného OLT, které by mohlo data dále přeposílat (po jejich uložení), by došlo k opětovnému provozu všech služeb. Umístění OLT jednotky útočníka pro odchycení dat ve vzestupném směru zobrazuje obr. 4.1. Bude-li brána v úvahu hlavní specifikace GPON sítě [53], (zabezpečení je dále specifikováno v [55]) zcela chybí OLT autentizace vůči ONU. Samotná autentizace ONU jednotky/jednotek je možná teprve po dosažení tzv. operačního stavu (Operational State) O5. Popis jednotlivých stavů pro jednotku ONU je detailně popsán v kapitole 4.4.2. Obecně lze tento stav shrnout jako konečný stav pro obousměrnou komunikaci mezi OLT a ONU. Díky chybějící OLT autentizaci by mohl na svém OLT obnovit fázi autentizace ONU. Všechny koncové jednotky obsahují dva unikátní parametry (ve vztahu k autentizaci): heslo

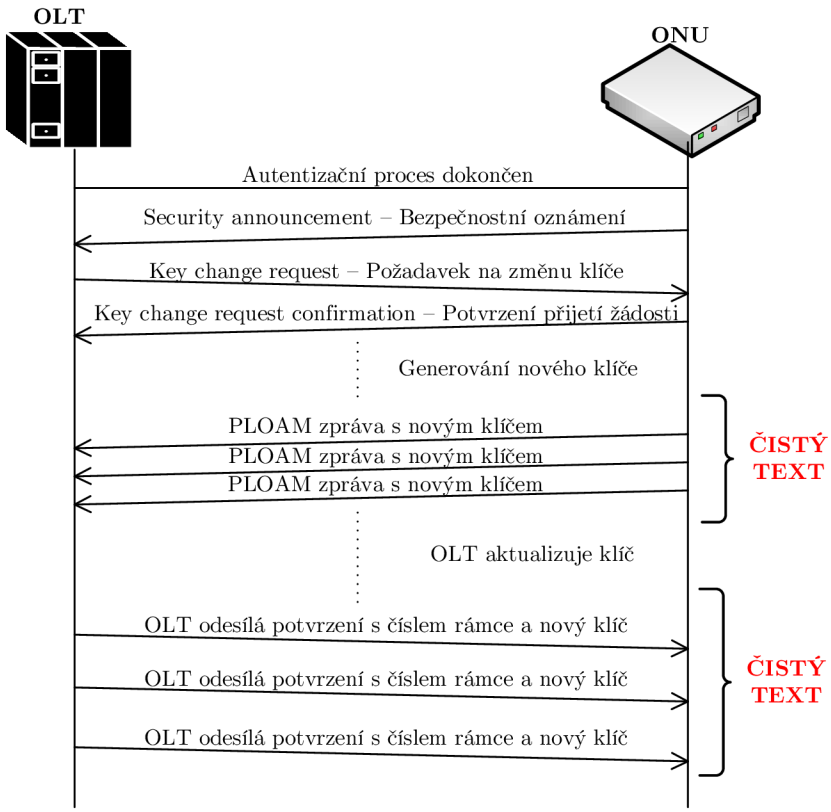


Obr. 4.2: Útočníkova OLT jednotka v distribuční síti

a šifrovací klíč. Nadřazená OLT jednotka může o tyto unikátní parametry kdykoliv požádat za pomocí PLOAM (Physical Layer OAM Operations, Administrations and Maintenance – správa fyzické vrstvy) zpráv. Pro získání hesla slouží PLOAM zpráva č. 7 Request_Password a pro šifrovací klíč PLOAM zpráva č. 11 Request_Password. Princip dotazu a odpovědi zobrazuje obr. 4.2. Klíčová část poskytovatele služeb je zabezpečit svou část sítě, nicméně z důvodu kaskádního zapojení splitterů není možné chránit objekty u koncových zákazníků, to je starostí majitele objektů. Poslední splittery bývají zpravidla víceportové i tam, kde není tak vysoký počet koncových zákazníků, neboť mohou sloužit k připojení budoucích zákazníků v daném místě (není vhodné využívat rozbočovací poměr, který je přesný – nemá rezervní port). Jedná se o tzv. flexibilní dynamiku ODN.

4.1.3 Správa hesel

Z výše uvedeného vyplývá, že OLT inicializuje aktivace a autentizace koncových jednotek. Základním požadavkem je dokončený aktivační proces po stav O5 a úspěšně dokončená autentizace ONU. Dále OLT inicializuje výměnu hesel pomocí (Security announcement) PLOAM zprávy následované požadavkem na výměnu šifrovacího klíče (Key change request). Požadavek na výměnu šifrovacího klíče musí být potvrzen zprávou Key change request confirmation. Dále proběhne samotné vygenerování klíče na základě unikátních informací dané jednotky ONU (např. sériové číslo, Alloc-ID aj.). Vygenerovaný klíč je přenášen třikrát v PLOAM zprávě (Encryption key). V případě použité fragmentace se přenáší více PLOAM zpráv. Aktuální doporučení spoléhá na charakter optického přenosu, tedy náročně odposlouchávaného přenosu a na složitost zapouzdření dat, a proto je klíč v nezabezpečené podobě (holé textové formě). Nehledě na rozdílné charaktery přenosu dat, sestupný směr je přená-



Obr. 4.3: Zprávy mezi OLT a ONU během výměny nového klíče

šen broadcastem, kdežto vzestupný směr je reprezentován unicastovým přenosem. Jakmile dojde ke zpracování příchozích zpráv obsahující nově vygenerovaný klíč, OLT odešle potvrzující zprávu s číslem rámce a přijatou podobu klíče (znovu jako holý text). Celou fázi zobrazuje obr. 4.3.

Útočník, při znalosti struktury rámce a schopnosti jej analyzovat v reálném čase, může získat identitu jiného uživatele (například k přenosu ilegálních dat). Poskytovatel služeb má k dispozici databázi (v OLT jednotce) o koncových zákaznicích. Jinými slovy, nahraje-li útočník citlivá nelegální data a kontrolní orgán bude chtít záznam IP adresy, pak ISP poskytne údaje zcela nevinného zákazníka, jemuž byla zcizena identita. Současné OLT jednotky spravují veškeré časové sloty pro veškeré ONU jednotky[2]. Na druhou stranu OLT jednotka nemůže poskytnout časové sloty pro komunikaci ONU jednotce, která byla autentizována se stejnými parametry jako druhá.

[2]Celkový počet koncových zákazníků není zcela relevantní, neboť OLT disponuje řádově lepším HW vybavením a lze je duplikovat.

4.1.4 Modifikované ONU

Modifikované ONU (v terminologii [53] známo jako „Rogue ONU“) je speciálním případem koncové stanice s pozměněným firmwarem. Podle principu komunikace v P2MP sítích, tedy za pomocí časových slotů (na základě obsahu pole BWmap), dochází k tomu, že Rogue ONU tyto časové sloty nerespektuje a vysílá svá data nepřetržitě v kontinuálním režimu. Následkem kontinuálního vysílání je, že ostatní jednotky (připojené na daný OLT slot) nemohou přenášet svá data, neboť dochází ke kolizím. Obecně není snadné detekovat takovouto jednotku v síti. Jednu z dostupných metod detekce Rogue ONU obsahuje specifikace [56], nicméně ta spoléhá na kompletní odpojení OLT jednotky a testování jednotlivých koncových splitterů. Časová náročnost detekce je značná, neboť je nezbytné kompletně odpojit OLT jednotku a postupně otestovat veškeré splittery na stranách koncových zákazníků. Představený nástroj je schopen detekce Rogue ONU pouze v sítích EPON, tedy pasivních optických sítích založených na přenosu Ethernetových rámců. Dílčím dokumentem k [53] je dokument [57], jenž slouží k základnímu popisu detekce Rogue ONU v GPON sítích, neudává však konkrétní postup pro alokaci této jednotky. Způsob detekce modifikované ONU je popsán v kapitole 4.5.5.

4.1.5 Porovnání šifrovacích algoritmů v PON

Zpravidla standardy podle ITU jsou založeny na šifrovacích algoritmech AES (Advanced Encryption Standard – standard pokročilého šifrování), nejčastěji na AES-128[3]. Výpis podporovaných šifrovacích algoritmů a výchozí konfiguraci zobrazuje tab. 4.1.

Tab. 4.1: Porovnání šifrovacích algoritmů v PON sítích

Standard	**Výchozí nastavení**	**Podporované algoritmy**
BPON	AES-128	DES, 3DEA, AES-128, AES-192, AES-256
GPON	AES-128	AES-128, AES-192, AES-256
XG-PON	AES-128	AES-128, AES-192, AES-256
NG-PON2	AES 128	AES-128, AES-192, AES-256
EPON	EAPoL	EAPoL
10G-EPON	AES-128	AES-128

Poskytovatel služeb může zvolit i silnější zabezpečení AES-192 nebo AES-256. Dnes nevyužívaný standard BPON (Broadband PON – širokopásmová pasivní optická síť) podporoval i starší techniky zabezpečení: DES (Digital Data Encryption

[3]Výchozí konfigurace.

Standard – standard pro zabezpečení přenášených dat) nebo 3DEA (Triple DES Algorithm – bloková šifra založená na šifrování DES). Oproti tomu, standard pocházející od IEEE – EPON (Ethernet PON – pasivní optická síť založená na přenosu Ethernet rámců) využívá EAPoL (Extensible Authentication Protocol over Local Area Network – rozšířený autentizační protokol) pro fázi výměny klíče a novější specifikace 10G-EPON (10G EPON – 10G EPON síť) využívá po vzoru ITU standardů techniku AES-128.

4.2 Zvýšení bezpečnosti v GPON sítích pomocí doby šíření signálu

Tato podkapitola se zabývá návrhem unikátního parametru, doby šíření signálu, pro zvýšení bezpečnosti bezpečnosti v GPON sítích[4]. Tento parametr bude dále použit při návrhu nového robustního bezpečnostního modelu (viz kapitola 4.3).

4.2.1 Dosavadní vývoj v oblasti zabezpečení PON sítí

Doposud bylo prezentováno několik vědeckých prací na téma bezpečnost pasivních optických sítí. Na druhou stranu většina z nich dává přednost standardům pocházejících od IEEE.

Autoři [58] se zaměřili obecně na detekci útočníka v síti, který se dostal k přenášenému signálu jednou z technik uvedených v kapitole. 4.1. Pro odhalení útočníka v síti je využíváno detekčního algoritmu ve spojení s FER (Frame Error Rate – chybovost rámců) parametrem pro každou koncovou jednotku. Obecně lze řešení shrnout následovně, nerespektuje-li útočník časové sloty, pak je jeho FER nejmenší v porovnání s ostatními uživateli na daném GPON portu. Jiné zdroje [59], [60] detailněji popisují bezpečnostní slabiny PON sítí a zabezpečovací metody pro sítě další generace. Jak již bylo zmíněno, EPON sítě byly často upřednostněny pro praktické nasazení, zejména díky známé zapouzdřovací metodě. Výstupy uvedené v [59] jsou zaměřeny na praktické hrozby jako jsou: odposlechy v síti, odepření služby pomocí DoS (Denial of Service – odepření služby), útok „maškarádou“ a tzv. zcizení služby. Práce [60] představuje jiné významné bezpečnostní riziko, využití odražených signálů. Koncept publikace je postaven na rozdělení signálu v optickém splitteru a následném měření odražených signálu na přenosovém médiu. Jelikož je známá struktura rámce, ve spojení s citlivým detektorem je možné zachytit a zpracovat přenášená data. Literatura [61] popisuje autentizační proces ONU jednotky. Nutno dodat, že tento autentizační proces je zcela odlišný od řešení pro GPON sítě.

[4]Unikátní parametr lze nasadit prakticky v libovolných optických sítích.

Autoři [62] se naopak zaměřují na řešení pro základní bezpečnostní rizika PON sítí: odposlechy v síti, odepření služby pomocí DoS, útok „maškarádou“ a útok přehráním. I pro oblast přístupových sítí byla zvažována možnost využití kvantové kryptografie [63], [64]. Cílovým standardem byl opět EPON s praktickou implementací kvantové kryptografie v kombinace s FBG (Fiber Bragg Grating – Bragovy mřížky) v sestupném směru. Další řešení analýzy pasivních sítí představuje OTDL (Optical Tapped Delay Line – optická zpožďovací linka), jenž využívá kombinaci přenášených informací ve velmi úzkých pásmech [65]. Každé pásmo má rozdílnou fázi v porovnání s předchozím vzorkem. Výsledný analyzátor kanálu nachází široké uplatnění jak ve všech typech pasivních optických sítích, tak i optických bezvláknových spojích.

Publikace [66] obsahuje vzájemný autentizační protokol založený na protokolu pro ustanovení klíče Diffie-Hellman. Jejich řešení chrání proti útokům: útok zopakováním, Meet-in-the-Middle, známé informace relace, poskytuje integritu dat aj. Prezentované řešení je navrženo pro EPON sítě a vyžaduje 8 exponenciálních operací, 2 symetrické zabezpečovací operace a 2 hash operace pro autentizační část a část ustanovení klíče. Řešení uvedené v kapitole 4.3 poskytuje shodné zabezpečení, ale vyžaduje menší počet operací.

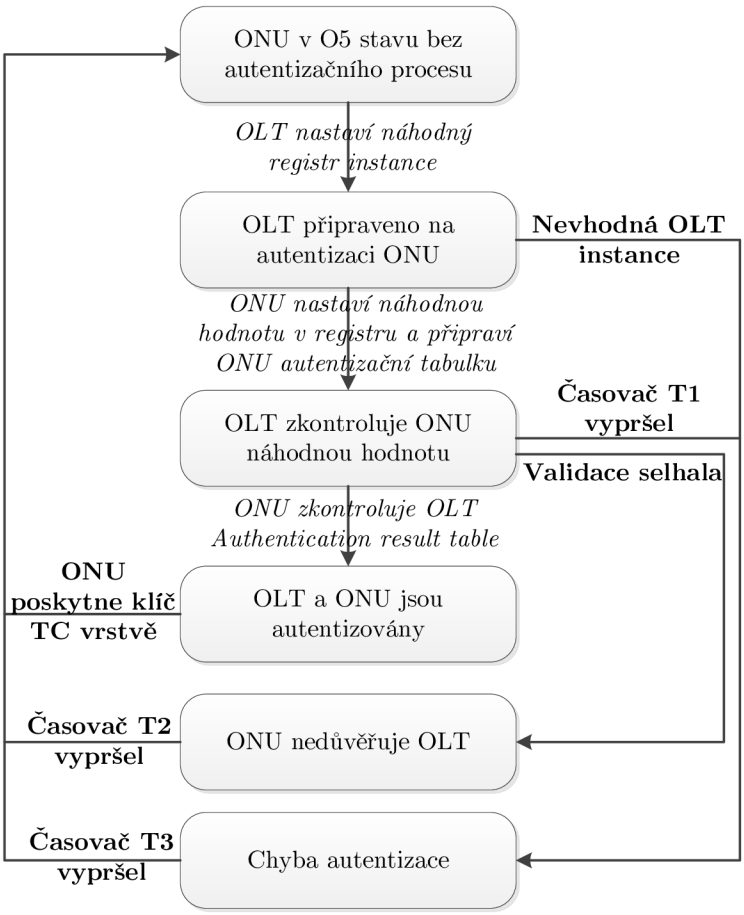
4.2.2 Autentizace a výměna klíče v GPON

Základní prerekvizitou je dosažení tzv. Operational state O5 (operačního stavu) koncové ONU jednotky. Kompletní popis jednotlivých stavů je součást kapitoly 4.4.2. Po dosažení tohoto stavu může jednotka komunikovat v obou směrech s řídicí jednotkou OLT. Výměna dat probíhá na základě časových slotů, které jsou plně v režii OLT jednotky. Přidělování těchto slotů může probíhat staticky nebo dynamicky[5].

Autentizační proces je zobrazen na obr. 4.4. Nejprve OLT inicializuje náhodnou instanci (uloží hodnotu instance do registru) a odešle PLOAM zprávu jednotce ONU, kterou chce autentizovat. Přijetím PLOAM zprávy ONU přechází do pending stavu (očekávající vyřízení), jinými slovy očekává další PLOAM zprávu s vygenerovaným číslem instance. Běžně mají ONU uloženou přednastavenou hodnotu pro autentizační proces, která je během pending stavu porovnána (na základě algoritmu). Nyní má ONU k dispozici pouze omezený čas (ve výchozí konfiguraci 3 sekundy), definován časovačem TO1[6], na odeslání odpovědi pro OLT. Nebude-li odpověď do této doby doručena, autentizační proces selže a je nezbytné jej zahájit od počátku (inicializací náhodné instance). V opačném případě je ONU autentizováno s OLT.

[5]Dynamické přidělování je záležitostí tzv. DBA (Dynamic Bandwidth Algorithm – algoritmus pro dynamické přidělení šířky pásma) algoritmů.

[6]Jehož hodnota může být libovolně upravena.



Obr. 4.4: Autentizační proces v GPON sítích

Po úspěšném dokončení autentizační fáze OLT[7] inicializuje fázi výměny klíče. Detaily výměny klíče jsou popsány v kapitole 4.1.3.

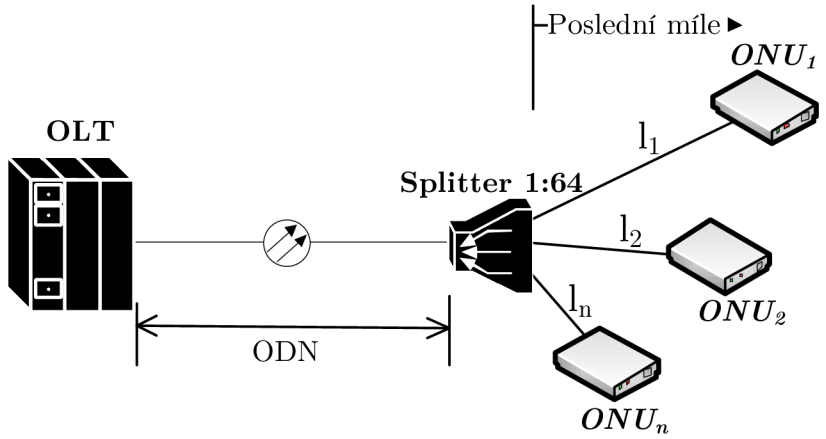
4.2.3 Návrh dodatečného parametru pro výměnu klíče

Předchozí podkapitoly se zabývaly autentizačním procesem a sestávajícím se z průběhu výměny klíče. Zásadním nedostatkem dnešních síti je, že výměna klíče je založena na předdefinovaném parametru (zpravidla sériovém čísle). Pokud by bylo uvažováno, že útočník by byl schopen odhalit algoritmus, který byl použit pro přidělování sériového čísla (lze i předpokládat, že poskytovatel služeb kupuje řádově stovky ONU koncových jednotek, pak je možné, že budou pocházet z jedné série a sériová čísla budou navazovat). Autoři [67] se zabývali bezpečnostními riziky v XG-PON za použití FPGA v reálném čase. Pokud bude brána v potaz výkonnost FPGA polí (více než 40 Gb/s), může být nalezení přiřazovací funkce sériového čísla

[7]Obrácená inicializace, tedy ONU, není možná.

koncovým jednotkám nalezena v krátkém čase, neboť první tři oktety identifikují výrobce (jsou neměnné).

Charakter pasivní optické sítě spoléhá na připojení koncových zákazníků pomocí pasivního splitteru. Základní typy ukončení optického vlákna jsou popsány v kapitole 3. Z výhledového hlediska se jeví nejvýhodněji (nejnákladnější) metoda FTTH, protože koncoví zákazníci nejsou „omezováni“ šířkou pásma metalických kabelů. Optické vlákno je ukončeno v bytě/domě zákazníka, čímž je dosaženo plně optické trasy, která je základní prerekvizitou nově navrženého parametru. Tento parametr je označován jako parametr síření signálu (dále zapisován/označován jako T_{prop}). Parametr specifikuje RTT (Round Trip Time – obousměrné zpoždění) čas přenosu dat mezi OLT a ONU. Charakter obecné pasivní optické sítě je zobrazen na obr. 4.5. Každý zákazník v reálné síti je připojen v rozdílné vzdálenosti od OLT jednotky, čehož využívá nový parametr T_{prop}. Ačkoli se zákazníci mohou nacházet ve stejné budově, ale v rozdílném podlaží, čímž je docíleno unikátní hodnoty T_{prop} pro každého z nich.

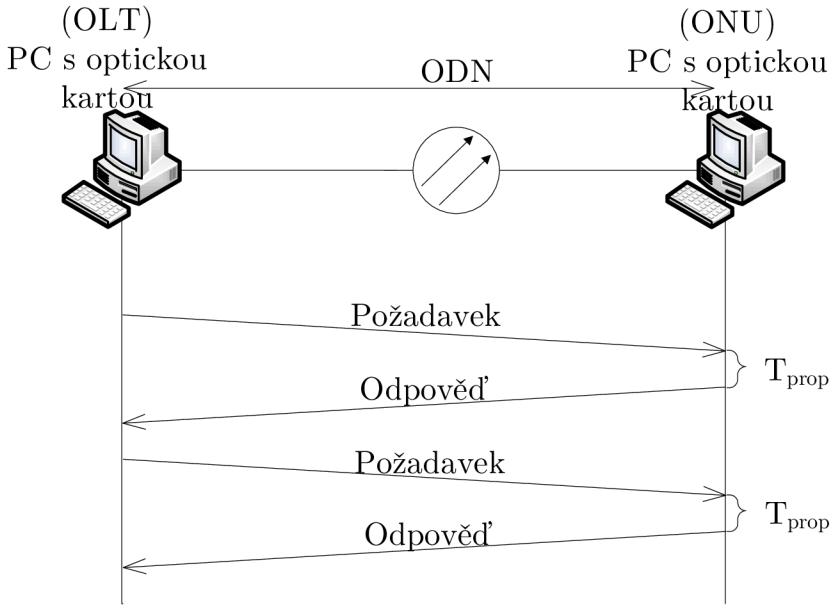


Obr. 4.5: Základní topologie GPON sítě

Standardní bezpečnostní model GPON sítí využívá pouze předkonfigurovaného tajemství (při výrobě). OLT může požádat o změnu klíče kdykoliv v průběhu komunikace (pouze s autentizovanou jednotkou), nicméně nový klíč bude vygenerován na základě uloženého tajemství nebo sériového čísla. Navržený model je unikátní, a to zejména díky absenci odesílání T_{prop} hodnoty nezabezpečenou distribuční sítí. Jinými slovy OLT i ONU znají dobu šíření na základě výměny zpráv, kde je specifikována časová známka odesílání/přijetí. Bude-li nezbytné dosáhnout zcela unikátní T_{prop}, kterou nelze předpovědět (ačkoli známý parametr T_{prop} nevede k odhalení klíče), může být specifikována dodatečná hodnota pomocí PLOAM zprávy 11 v sestupném směru – Request Key – který bude připočten/odečten od naměřené hodnoty T_{prop}.

4.2.4 Experimentální ověření parametru šíření

Cílem experimentálního ověření bylo potvrzení obousměrné komunikace mezi OLT a ONU s časovými razítky pro datové jednotky a jejich vzájemný vztah (z hlediska doby šíření v obou směrech). Dostupné GPON komponenty neposkytují žádné API (Application Programming Interface – rozhraní pro programování aplikací). Bude-li uvažováno, že OLT a ONU jednotky využívají pro přenos dat distribuční síť, není nezbytné provádět měření přímo na aktivních GPON komponentech (OLT a ONU), protože dochází k přenosu pouze Ethernetovských rámců zapouzdřených do GTC rámců [53]. Alternativní schéma k GPON síti je zobrazeno na obr. 4.6.



Obr. 4.6: Alternativní schéma pro měření T_{prop} parametru

Reálná síť sestává z jednovidových vláken, splitteru a aktivních komponent. Experimentální ověření proběhlo za pomocí dvou PC s optickými kartami (Broadcom NetXreme II BCM57711[8]) s SFP (Small Form-factor Pluggable – zásuvný SFP modul) slotem, SFP (Finisar FTLX1671D3BC) moduly, splittery s malými dělicími poměry a různě dlouhými jednovidovými vlákny připojené za splitter 1:4. V porovnání s reálnými trasami bylo použito splitteru s malým dělicím poměrem, neboť vyšší dělicí poměr nemá vliv na dobu šíření signálu, ale na konečný útlum trasy.

[8]Za zapůjčení optických karet bych rád poděkoval Ing. Josefu Vojtěchovi, Ph.D. ze sdružení CESNET.

Měření T_{prop}

Jak bylo zmíněno, zpočátku bylo nezbytné navrhnout náhradní zapojení adekvátní reálné síti. Dalším krokem bylo navrhnout metodologii měření T_{prop} parametru. Bude-li brána v potaz síť založena na protokolu Ethernet, pak by bylo možné využít příkaz `ping` v CMD (Command Line – příkazový řádek). Nevýhodou příkazu `ping` je, že využívá ICMP (Internet Control Message Protocol – protokol pro diagnostiku sítí), který pracuje na 4. vrstvě modelu ISO/OSI (International Organization for Standardization/Open Systems Interconnection – sedmi-vrstvý referenční model ISO/OSI), nicméně GPON sítě pracují na prvních dvou vrstvách modelu ISO/OSI. Z toho důvodu bylo využito protokolu ARP (Address Resolution Protocol – služební protokol pro překlad adres) za pomocí příkazu `arping` s fyzickou adresou optické karty. Odpovědi byly zaznamenávány v ms, což je pro stanovení T_{prop} parametru nedostačující. Z tohoto důvodu bylo využito síťového analyzátoru Wireshark na obou počítačích. Díky kompletnímu uchování datových jednotek, byla uložena i časová razítka každého rámce (přesnost Wireshark nástroje udávána v µs). Měření každého požadavku (reprezentováno příkazem `arping`) bylo zopakováno 9× a pro post-processing bylo uvažováno vždy stejné pořadí rámců. Pro stanovení T_{prop} byly uvažovány 2., 3. a 4. rámce (doba odeslání a přijetí rámce).

V rámci měření byly otestovány tři různé délky distribuční sítě 1, 20 a 40 km, celkové délky optického vlákna. GPON sítě limitují distribuční síť na 20 km z důvodu omezení celkového útlumu a zajištění časové synchronizace. Díky nízkému dělicímu poměru bylo možné provést měření v rámci 40km distribuční síti. Pro dvojnásobnou délku distribuční sítě byly očekávány dvojnásobné hodnoty T_{prop} parametru. Naměřené výsledky shrnuje tab. 4.2.

Tab. 4.2: Naměřené hodnoty T_{prop} parametru v různých vzdálenostech ODN

Délka distribuční sítě [km]	T_{prop} **A→B [µs]**	T_{prop} **B→A [µs]**
1	278	278
20	435	435
40	594	594

Z tab. 4.2 je zřejmé, že bude dosaženo stejné hodnoty parametru T_{prop} v obou směrech, čímž byla dokázána funkčnost alternativního zapojení. Zpočátku probíhalo měření pomocí příkazu `arping`, kde bylo dosaženo přesnosti $\approx 1{\cdot}10^{-5}$. Z naměřených hodnot lze odvodit přesnost v řádu stovek metrů pro každou ONU. Hodnoty T_{prop} pro distribuční sítě o délce 20 a 40 km jsou ≈158 µs a ≈317 µs. Rychlost šíření pro 1 km jednovidového optického vlákna je ≈8 µs (včetně doby šíření a doby zpracování).

Na základě této znalosti lze odvodit, že naměřená hodnota 278 µs obsahuje dobu zpracování signálu odpovídající ≈270 µs. Finální rozlišení zajišťuje rozdílné hodnoty T_{prop} pro zákazníky na rozdílných podlažích (optické vlákno je přivedeno do bytu/domu zákazníka včetně rezervy). Díky kombinaci uloženého tajemství (nebo použití sériového čísla) a unikátního parametru T_{prop} může být použito tohoto parametru ve fázi výměny klíče (ve fázi generování klíče) pro zvýšení bezpečnosti v GPON sítích.

Pokud bude možno měřit parametr T_{prop} v „ns“, pak by bylo docíleno zcela unikátní hodnoty T_{prop} pro každého koncového zákazníka, včetně zákazníků nacházejících se na stejném podlaží budovy. Výsledky měření byly publikovány v [68].

4.3 Robustní model zabezpečení GPON sítí

Předchozí podkapitola se zabývala návrhem unikátního parametru pro zvýšení bezpečnosti GPON sítí. V této podkapitole bude nadále využíváno tohoto parametru v robustním modelu zabezpečení datové komunikace.

4.3.1 Systémový model

Navržený model předpokládá následující části:

- OLT – je řízeno poskytovatelem služeb je umístěno v CO (Central Office – centrální ústředí poskytovatele) části přístupové sítě a využívá hraniční prvky pro připojení/přenášení dat do celosvětové sítě Internet. OLT je zodpovědné za správu optických parametrů (výkonová úroveň, doba trvání rámce atd.) v přístupové síti, rovněž poskytuje autentizaci ONU jednotek a zajišťuje komunikaci s ONU jednotkami.
- technik (T) – nastavuje ONU jednotky v přístupové síti. Zpravidla nahrává kryptografické parametry a základní konfiguraci do ONU.
- ONU – veškeré koncové jednotky jsou spravovány technikem a poskytují konverzi mezi optickým a elektrickým signálem (a obráceně) na straně zákazníků. Rovněž zabezpečuje obousměrnou autentizaci a zajišťuje komunikaci v přístupové síti[9].
- splitter – je pasivní optické zařízení, které slouží k připojení koncových zákazníků. Zpravidla je stále považováno za součást distribuční sítě.

[9] Od/k zákazníkům z jejich domácí LAN (Local Area Network – lokální síť).

4.3.2 Použitá kryptografie

Navržené řešení, založené na moderních kryptografických metodách, poskytuje vzájemnou autentizaci (ONU a OLT) se zabezpečenou výměnou klíčů a efektivní zabezpečení přenášených dat v obou směrech, aby bylo docíleno komplexní bezpečnosti v GPON sítích.

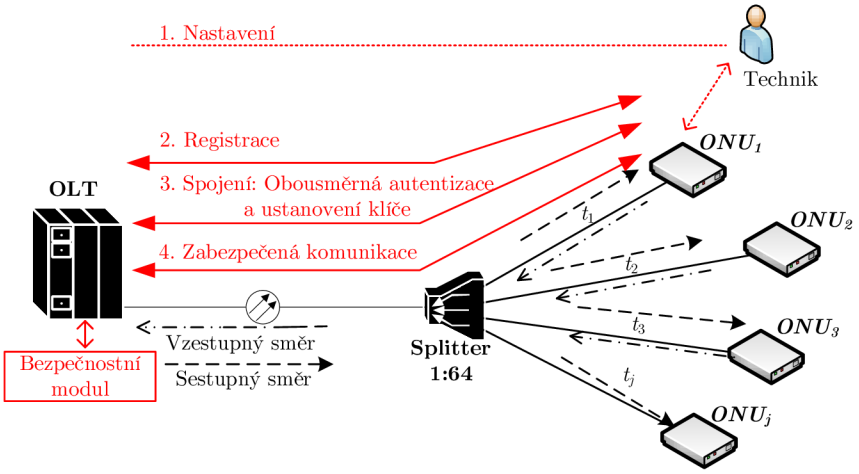
Vzájemná autentizace je zajištěna použitím tajné hodnoty a T_{prop} parametru, který je unikátní pro každou dvojici OLT a ONU. Tajné parametry jsou ustanovené během registrace ONU. Popis měření T_{prop} parametru je v kapitole 4.2.4.

Navržený protokol pro ustanovení klíče je založen na ECDH (Elliptic Curve Diffie–Hellman – Diffieho-Hellmanův protokol s využitím eliptických křivek) protokolu, jenž je modifikován na protokol SPEKE (Simple Password Exponential Key Exchange – metoda ustanovení klíče s využitím modulárního umocňování a sdíleného hesla) [69]. Generátor G není vytvořen ve funkci jako u standardů IEEE P1363.2 a ISO/IEC 11770-4, ale bylo použito sdílené tajemství ve funkci HMAC (Keyed-Hash Message Authentication Code – typ autentizačního kódu zprávy), která kontroluje autentičnost a integritu vygenerovaných relačních tajných klíčů a všech parametrů během „fáze spojení“ (Join fáze).

Datová komunikace je zabezpečena pomocí šifry AES, která poskytuje adekvátní rychlost k rychlostem datové komunikace v GPON sítích.

4.3.3 Fáze řešení

Navržené řešení je rozděleno do 4 hlavních fází: setup (nastavení), registration (registrace), join (spojení) a zabezpečená komunikace. Jednotlivé fáze jsou zobrazeny na obr. 4.7.



Obr. 4.7: Schéma navrženého řešení zabezpečení

Nastavení

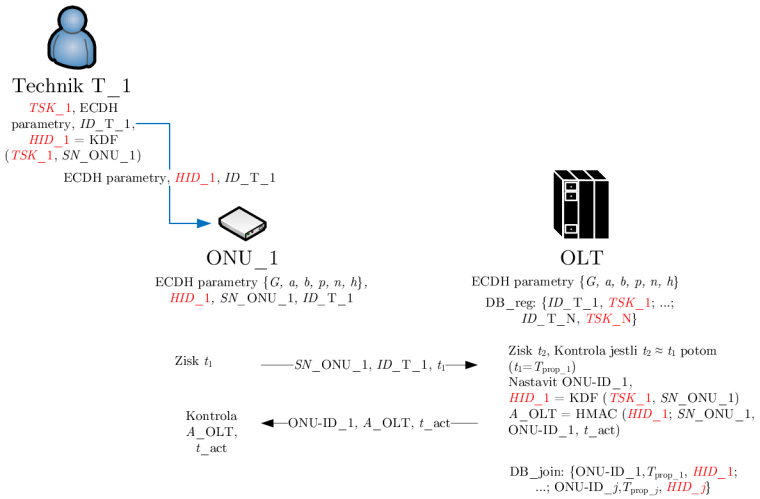
Poskytovatel služeb v rámci této fáze vygeneruje kryptografické parametry jako jsou: hlavní tajný klíč (MSK), tajný klíč technika a ECDH parametry. Pro ECDH parametry je nezbytné vybrat vhodnou křivku. Navržené řešení využívá křivku Curve25519, kterou jako první uveřejnil Daniel J. Bernstein v roce 2005 [70]. Tato křivka je navržena pro ECDH a poskytuje 128bit zabezpečení. Hlavní tajný klíč $MSK \in \{0,1\}^{256}$ je náhodně generován a je znám pouze poskytovateli služeb, z tohoto důvodu by měl být uchován v zabezpečeném úložišti (na obr. 4.7 zobrazeno jako bezpečnostní modul). Tajný klíč technika $TSK\_n \in \{0,1\}^{256}$ je odvozován za použití KDF (Key Derivation Function – funkce odvození klíče), např. HMAC s SHA-2 (Secure Hash Algorithm – rozšířená hashovací funkce). Klíče jsou vypočteny jako $TSK\_n{=}KDF(MSK, ID\_T\_n)$, kde ID_T_n je unikátní identita n-technika. OLT ukládá pár ID_T_n, TSK_n v zabezpečeném úložišti. Dále bude tento pár označován jako registrační databáze (DB_reg). Každý technik T_n vlastní TSK_n, ECDH parametry a ID_T_n. Technik je schopen nastavovat a konfigurovat libovolné ONU_j.

Registrace

Kryptografické detaily registrační fáze jsou zobrazeny na obr. 4.8. Hlavním cílem této fáze je nastavení předsdílených tajemství, doby šíření signálu a registrace ONU k OLT. Registrační fáze může být rozdělena do dvou kroků. V prvním kroku n-technik nakonfiguruje i-ONU a v druhém kroku i-ONU komunikuje s OLT přes GPON síť (distribuční síť). Oba kroky jsou detailně popsány níže:

1. Předpokládejme, že technik T_n nastaví a nakonfiguruje ONU_i. Dojde k přečtení sériového čísla ONU_i (SN_ONU_i) a výpočtu $HID_i = KDF(TSK\_n, SN\_ONU\_i)$ za použití jeho/jejího tajného klíče TSK_n. Poté T_n nahraje do ONU_i ECDH parametry, HID_i a jeho/její identifikační číslo ID_T_n. Tajný parametr HID_i je použit pro autentizaci OLT v této fázi a pro autentizaci ONU_i v join fázi.
2. V tomto kroku se ONU nachází v operačním stavu (O5). ONU_i se připojí do sítě (pouze ve stavu O5 je možno komunikovat obousměrně) a odešle své SN_ONU_i, ID_T_n a t_1, kde t_1 je naměřená hodnota propagačního zpoždění na straně ONU. Po přijetí dat od ONU_i, OLT zahájí měření t_2 (doba propagačního šíření T_{prop}) a ověří, jestli si jsou hodnoty rovny. Ze znalosti ID_T_n, OLT nalezne TSK_n v DB_reg databázi a vypočte $HID\_i = KDF(TSK\_n, SN\_ONU\_i)$. OLT nastaví $ONU{-}ID\_i$ a uchová $ONU-ID\_i$, T_{prop_i}, HID_i do DB_join databáze, která je využita při join fázi. Dále OLT dostane aktuální časovou známku t_act a vypočte

A_OLT=HMAC $(HID\_i, SN\_ONU\_i, ONU-UD\_i, t\_act)$ a všesměrově odešle $ONU-ID\_i$ a t_act. $ONU-i$ musí ověřit čerstvost (freshness) t_act a A_OLT za pomocí výpočtu hodnoty hashe z přijatých parametrů.



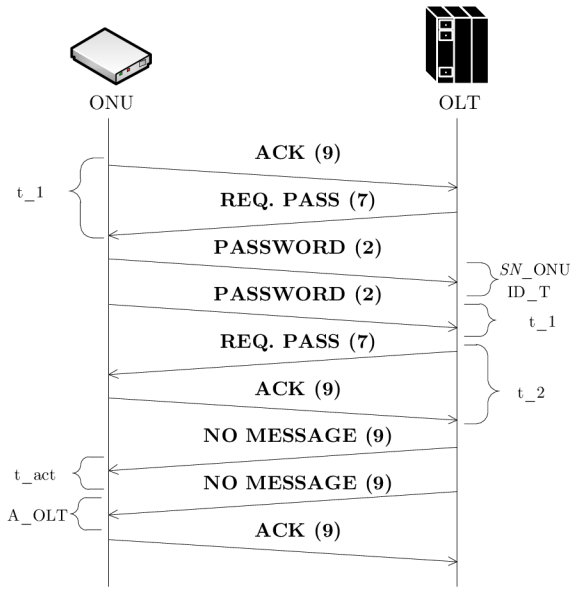
Obr. 4.8: Kryptografické detaily registrační fáze

PLOAM zprávy během fáze registrace

Nový model vychází ze zcela nového přístupu k autentizaci a přístupu k zabezpečení dat v GPON sítích. Má-li být nový model nasazen, je nezbytné zajistit co nejméně změn v přenosové vrstvě a použitých zpráv PLOAM. Z tohoto důvodu byl kladen důraz na použití již existujících PLOAM zpráv, čímž bude zachována kompatibilita s GPON sítěmi všech výrobců. Jakmile ONU dosáhne operačního stavu (O5), poté je možné přenášet data v obou směrech.

Nejprve odešle ONU zprávu ACK (PLOAM zpráva č. 9) pro zahájení měření parametru t_1. OLT odpovídá zprávou Request_Password (PLOAM zpráva č. 7) konkrétní ONU za použití identifikátoru ONU-ID. Pro identifikaci ONU-ID slouží první oktet v PLOAM zprávě. Funkci zpracovávat PLOAM zprávy mají veškeré ONU jednotky, bez ohledu na to v jakém stavu se aktuálně nacházejí. Zpráva Request_Password obsahuje nespecifikovanou podobu pro 3.–12. oktet [53]. Díky tomuto je možné specifikovat SN_ONU požadavek. Jakmile ONU zná čas odeslání a přijetí, je možné vypočítat t_1, jakožto parametr šíření signálu. Velikost rámce je neměnná a definována v [53] jako 125 µs. Obdobně jako ONU vypočítalo parametr t_1, vypočte OLT svůj parametr t_2, které si jsou rovny. Zde je nutno poznamenat, že OLT jednotka v aktuální konfiguraci v reálných sítích nevypočítává tento parametr, proto by bylo nezbytné implementovat funkci, která by tuto dobu umožnila stanovit, neboť

časy přijetí a odeslání rámců jsou známy. Následně ONU poskytne parametry pro registrační proces: ID_t, t_1 a SN_ONU obsažených v PLOAM zprávě Password (PLOAM zpráva č. 2). OLT uchová přijatá data pro konkrétní ONU (identifikovanou pomocí ONU-ID v PLOAM zprávách). Nyní OLT odešle své parametry pro konkrétní ONU s (ONU-ID): A_OLT a t_act odeslaných ve zprávě No_Message (PLOAM zpráva č. 9). Celkový počet těchto zpráv závisí na velikostech parametrů, které jsou přenášeny. ONU jednotka očekává 3 parametry a po jejich přijetí odpovídá zprávou ACK. Výše uvedené detaily obsahuje obr. 4.9[10].



Obr. 4.9: Použité PLOAM zprávy během registrační fáze v navrženém řešení

Fáze spojení

Tato fáze poskytuje informace o ustanovení klíče a autentizaci. Základní koncepci této fáze zobrazuje obr. 4.10. Unikátní parametr, propagační zpoždění, který je sdílen mezi ONU a OLT bylo ustanoveno v rámci předchozí fáze. Parametry ECDH, ONU--ID_i a HID_i byly ustanoveny v registrační fázi.

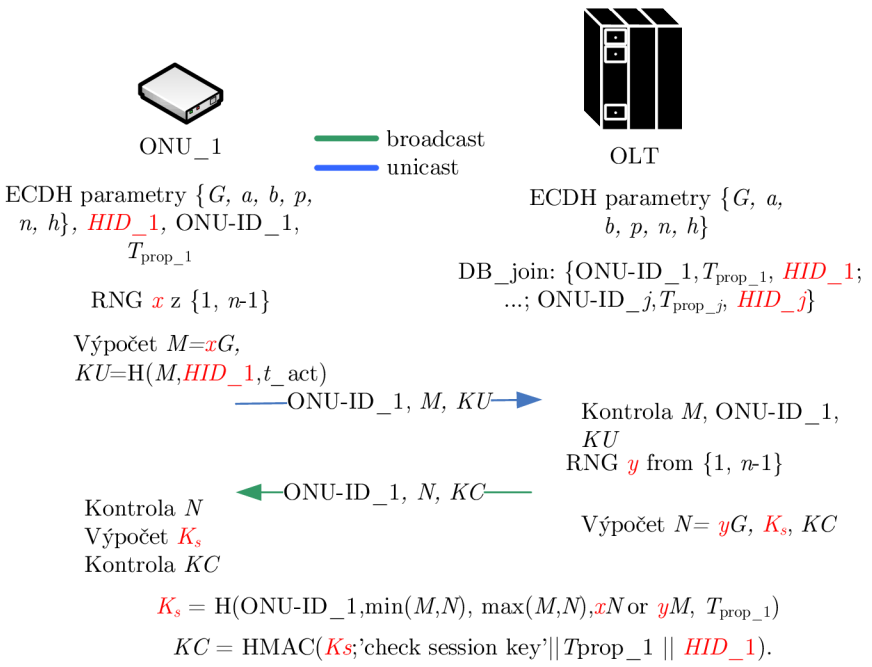
Join fáze probíhá mezi i-ONU a OLT základní kryptografické detaily lze shrnout následovně:

- Základním předpokladem je, že parametry ECDH a T_{prop_i} jsou shodné na obou stranách (ONU a OLT).
- ONU_i vygeneruje náhodnou tajnou hodnotu $x \in (1, q-1)$ a vypočte veřejné ECDH parametry $M = xG$. Poté ONU_i vypočte uživatelský autentizační tag

[10]Pro zachování terminologie je označení zasílaných zpráv v angličtině.

$KU = H(M, HID\_i, t\_act)$, kde je t_act aktuální časovou známkou, což zabrání potenciálnímu „reply útoku“, H je hashovací funkce (např. SHA2). Identity od ONU$_i$ (ONU-ID$_i$), M a KU jsou odeslány OLT jednotce.

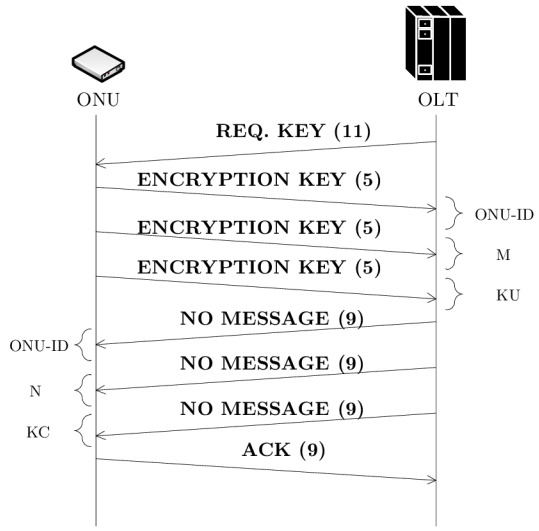
- OLT přijme identity od konkrétního ONU-ID$_i$, KU a M. Nejprve OLT zkontroluje identifikátor ONU-ID$_i$, jestli se nachází v seznamu aktivních zařízení. Pokud ONU-ID$_i$ je nalezena, dojde k uložení parametrů HID_i a T_{prop_i}. Dále OLT zkontroluje KU vypočtením KU' za použití stejné funkce. Jestliže KU' neodpovídá KU, pak je fáze spojení zastavena. Následně OLT vypočte relační klíč relace $K_s = H(ONU - ID_i, min(N, M), max(N, M), M^y, T_{prop\_i})$. Tento klíč je uložen na bezpečném místě v OLT. Navíc OLT vypočte potvrzovací hodnotu klíče $KC = HMAC(K_S, 'checksessionkey' \| T_{prop} \| HID\_i)$, kde HMAC je funkce pro výpočet autentizační kódu při využití tajného klíče a funkce hash (např. HMAC-SHA256). OLT odešle ONU-ID$_i$, N a KC pro všechny ONU všesměrovým kanálem.
- ONU$_i$ přijme ONU-ID$_i$, N a KC všesměrovým kanálem. ONU$_i$ nejprve ověří, jestliže zpráva s ONU-ID$_i$ je adresována právě této jednotce. Poté ONU$_i$ vypočte klíče relace $K_s = H(ONU - ID_i, min(N, M), max(N, M), N^X, T_{prop\_i})$ a zkontroluje KC přepočítáním $KC = HMAC(K_S, 'checksessionkey' \| T_{prop} \| HID\_i)$. Jestliže přepočtený KC je stejný, pak ONU$_i$ a OLT mohou zahájit zabezpečenou komunikaci za použití ustanovení relačního klíče K_S. Jinak je tajný klíč zahozen.



Obr. 4.10: Kryptografické detaily join fáze

PLOAM zprávy během join fáze

OLT odešle zprávu Request_Key (PLOAM zpráva č. 11) s konkrétní ONU-ID pro danou ONU. ONU s odpovídajícím ONU-ID odpovídá zprávou Encryption_Key (PLOAM zpráva č. 5), která obsahuje ONU-ID parametr. Předpokládá se použití posledních osmi LSB (Low Significant Bit – nejméně významný bit) pro ONU-ID. Zpráva Encryption_Key obsahuje parametr M (rozdělen do dvou rámců). Čtvrtá a pátá zpráva obsahuje KU parametr. OLT zpracuje přijaté parametry od ONU a poskytne následující parametry: ONU-ID, N a KC pro ONU s konkrétní ONU-ID za použití zprávy No_Message (PLOAM zpráva č. 9). Jakmile ONU přijme všechny parametry, pak odešle ACK zprávu (PLOAM zpráva č. 9). Diagram odeslaných zpráv je reprezentován na obr. 4.11.



Obr. 4.11: Použité PLOAM zprávy ve fázi join

Zabezpečená komunikace

Komunikace v sestupném a vzestupném směru je zabezpečena pomocí tajného klíče relace K_S, který byl ustanoven v předchozí fázi. V této fázi je použito rychlého šifrování (např. AES v GCM módu). Navržený algoritmus spoléhá na rychlé šifrování AES metodu s časovou známkou, popsáno v [71]. Během join fáze může dojít k přerušení služeb (ztráty signálu). Například k dispozici je časovač TO2 s hodnotou 100 ms, jestliže ONU ztratí signál (více než jeden Psync část rámce), pak je k dispozici právě 100 ms na obnovu synchronizace. Obnoví-li spojení během 100 ms, poté je ONU umožněno zůstat ve stejném stavu, jinak se ONU vrací do stavu O1.

V případě výpadku spojení (vlivem přerušení dodávky elektrické energie) musí každá ONU začít od prvního stavu O1, neboť není možné spustit časovač TO2.

4.3.4 Bezpečnostní analýza

Tato část pojednává o bezpečnostních rizicích v GPON sítích. Předpokládá se, že útočník (A) má přístup ke komunikaci a je schopen naslouchat zprávám v obou směrech, rovněž se předpokládá aktivní schopnost přečíst, modifikovat a vytvořit novou zprávu. Dále útočníkovo ONU se bude snažit napodobit ostatní ONU a získat jejich data. Kromě toho se útočníkova ONU jednotka pokouší provést falešnou autentizaci a ustanovení klíče. Přesto se však nepředpokládá, že by měl útočník k dispozici výpočetní výkon, který by mu/jí umožnil prolomit běžné kryptografické metody, jenž jsou dnes považovány za bezpečné.

Řešení zabraňuje odposlechu

Útočník, který odposlouchává komunikaci mezi ONU a OLT během join fáze není schopen získat tajný klíč, jenž je použit pro zabezpečení datové komunikace ve fázi zabezpečené komunikace. Útočník by musel znát tajné ECDH parametry x nebo y a T_{prop} parametr pro získání tajného klíče. Zároveň by musel vyřešit Diffie-Hellman problém a znát platný T_{prop} parametr pro získání tajného klíče. Útočník není schopen extrahovat klíč z šifrovaného textu během odposlechu komunikačního kanálu. Bezpečnost komunikace je založena na symetrické kryptografii (AES-128).

Řešení zabraňuje napodobování cizích ONU

Útočník snažící se napodobit jinou ONU_i s ONU-ID_i musí znát tajný parametr HID_i, aby byl autentizován s OLT. OLT ukládá HID_i, které jsou bezpečně uloženy s ostatními ONU-ID_i a kontroluje KU od ONU za účelem přepočítání hash hodnoty z M, HID_i a aktuálního času. Parametr HID_i může být vypočten pouze za použití technikova tajného klíče (TSK_n), který je uložen v zabezpečeném modulu na straně OLT a zabezpečném modulu od techniků.

Řešení zabraňuje napodobování cizích OLT

Útočník, jenž se snaží napodobit OLT jednotku, musí znát tajný parametr HID_i, technikův tajný klíč (TSK_n), nebo hlavní tajný klíč. Hodnota HMAC (A_OLT) s HID_i, SN_ONU_i, ONU-ID_i a t_act jsou použity pro autentizaci OLT na straně ONU během registrační fáze. Během join fáze je použita hodnota HMAC (KC).

Řešení zabraňuje útoku opakování zpráv

Jestliže útočník zachytí join zprávy, které jsou odesílány od ONU_i k OLT, poté může zkusit opětovné odeslání této zprávy v budoucnu. Nicméně hash parametr KU je vypočten z aktuálního časového razítka a tajné hodnoty HID_i, tedy bez tajné hodnoty HID_i není útočník schopen obnovit tuto zprávu. Rovněž i registrační fáze je zabezpečena aktuální časovou známkou pro výpočet hodnoty A_OLT.

Řešení zabraňuje útoku podvrhu/modifikaci dat

Integrita dat během registrační fáze je zabezpečena hodnotou A_OLT, která je vypočtena ze všech základních parametrů. Jestliže jsou data porušována/narušována během join fáze, potom parametr KC není shodný na straně ONU_i i OLT a ONU_i nepoužije ustanovený klíč. HMAC funkce je bezpečná, pokud modifikace KC bez znalosti x nebo y, HID_i a T_{prop} je velmi náročná.

Řešení zabraňuje on-line slovníkovému útoku

Útočník bez znalosti HID_i není schopen dokončit join fázi a ustanovit bezpečný klíč. Špatná HID_i hodnota ihned zastaví join fázi. Tudíž, útočník má pouze jedinou možnost odhadnout HID_i hodnotu.

Řešení zabraňuje off-line slovníkovému útoku

Pokud útočník zachytí join zprávy a poté se pokusí odhadnout HID_i započne znovuvypočtení KC. Nicméně KC je vypočten za použití tajného klíče K_S, který je odvozován z ECDH tajné hodnoty (y). Útočník není schopen přepočítat KC bez y. Extrakce HID_i z A_OLT nebo KU je velmi náročná kvůli zabezpečení hashe a HMAC funkcí.

Řešení chrání proti úniku slabého hesla

V případě, že útočník zná hodnotu HID_i, která je reprezentována tajnou hodnotou v tomto řešení, potom útočník není schopen vypočítat tajné klíče, které jsou již používány, bez znalostí tajných hodnot x a/nebo y. Pro získání těchto parametrů ze zpráv přenášených v rámci protokolu pro ustanovení klíče by musel útočník být schopen vyřešit problém diskrétního logaritmu.

4.3.5 Výkonnostní zhodnocení a výsledky

Tato část se zabývá ohodnocením (výkonnostním) a porovnáním s ostatními souvisejícími pracemi. Dále byla provedena experimentální implementace a ověřena funkčnost a časová náročnost řešení.

Časová náročnost řešení

Navržené řešení registrační a join fáze rozšiřuje ITU-T G.984 standard o několik kryptografických metod. V registrační fázi ONU vypočítá 1 HMAC operaci a OLT vypočítá rovněž 1 HMAC operaci spolu s 1 hash operací. Během join fáze ONU spočítá 2 hash operace, 1 HMAC operaci a ECDH operaci. Join fáze je symetrická, čímž OLT provede stejné výpočty jako ONU.

Cílem bylo porovnat vlastní řešení s již existujícím řešením od autorů [72]. Autentizace a fáze ustanovení klíče od [72] (dále jen YQZ schéma) mohou být porovnány s vlastní registrační a join fází. Kromě toho, se předpokládá pouze jedno násobení bodu na eliptické křivce, což zabere přibližně stejný čas jako modulární umocňování exponenciální operace použité v YQZ schématu. Autentizace a ustanovení klíče v YQZ zabere 10 modulárních exponenciálních operací, 6 modulárních násobení, 2 HMAC operace a 2 symetrické šifrovací operace. Registrační a join fáze v navrženém řešení vyžadují 4 operace násobení bodů na eliptické křivce, 4 HMAC operace a 5 hash operací. Z toho vyplývá, že navržené řešení potřebuje časově méně náročné operace jako: násobení bodu na eliptické křivce, umocňování a násobení, potom YQZ schéma ale přidává několik základních operací jako 2 HMAC funkce a 5 hash operací.

Experimentální implementace

Během implementace vlastního řešení byla měřena časová náročnost použitých metod v registrační a join fázi. Princip měření T_{prop} parametru vychází z kapitoly 4.2.4.

Měření kryptografického řešení

Pro ověření kryptografických metod bylo použito programovacího jazyka Java. Jelikož není možné implementovat vlastní řešení do jednotek OLT a ONU (nemají k dispozici odemčené API), bylo nutno využít embedded zařízení s 700 MHz CPU (Central Processor Unit – centrální procesorová jednotka) a 512 MB RAM (Random Access Memory – paměť s náhodným přístupem) s operačním systémem Linux Debian, které reprezentovalo ONU jednotku. OLT bylo zastoupeno PC (Personal Computer – osobní počítač) 2,53 GHz CPU a 8 GB RAM s operačním systémem Windows 7. Výsledky měření zobrazuje tab. 4.3, která obsahuje čas běhu programu kryptografických operací na simulovaných zařízeních OLT a ONU během registrační

Tab. 4.3: Výsledné doby běhu programu pro vlastní řešení

Fáze	**Čas pro ONU [ms]**	**Čas pro OLT [ms]**	**Celkový čas [ms]**
Registrace	3,6	0,4	4,0
Join	42,8	2,7	45,5

a join fáze. Prezentované výsledky jsou zprůměrované hodnoty (100 měření) celkového chodu programu v jednotlivých fázích. Registrace vyžadovala ≈4 ms. Nicméně ONU vyžadovalo 42,8 ms a OLT 2,7 ms v join fázi.

V praxi OLT může vykonávat registrační a join fázi s více ONU jednotkami (např. 64 ONU), pak OLT potřebuje ≈198,4 ms pro zabezpečovací operace v obou fázích. ONU vyžaduje ≈46,4 ms pro obě fáze.

Vlastní bezpečnostní řešení na základě měření propagačního zpoždění v GPON sítích a bezpečnostní analýza byly prezentovány v [73], [74] a [75].

4.4 Simulace a měření komunikace v GPON sítích

Jedná se o zcela novou oblast pasivních optických sítí, která není příliš probádána, doposud existuje velmi málo publikací, které se zabývají vyššími vrstvami v PON sítích [76]. Nicméně tato publikace popisuje pouze dostupné metody zapouzdření (formáty rámců) a vliv jejich velikosti na efektivnost přenosu. Autoři zároveň nezahrnuli do své práce oblast časování, která je pro koncové jednotky zcela klíčová, neboť vzestupný směr (od ONU k OLT) je řízen pomocí časového dělení. Dojde-li k výpadku napájení, mohou se poslední zákazníci připojit v závislosti na velikosti sítě od desítek minut po řádově hodiny.

4.4.1 Dosavadní vývoj pro simulace a měření PON sítí

Dosavadní vývoj pro měření v PON sítích se zaměřuje především na fyzickou vrstvu sítí. Veškeré základy měření pasivních optických sítí pomocí metody OTDR (Optical Time Domain Relflectometry – reflektometrická měřicí metoda) poskytuje článek [77]. Článek je zaměřen na ukázkové scénáře, umístění měřicího přístroje i analýzu možných výsledků měření. Jiná publikace navazuje na měření a nyní využívá měřicí přistroj BOTDR (Brillouin Optical Time Domain Relflectometry – Brillouinova reflektometrická měřicí metoda) [78]. Autoři [79] se zaměřují na tři způsoby měření během dílčích fází výstavby pasivní sítě: měření po instalaci trasy, měření během provozu sítě a poslední měření pro detekci chyb na fyzické vrstvě. Měření pro sítě NG-PON2 založených na TDM dělení je věnována značná pozornost v [80].

Na druhou stranu publikace zabývající se přenosovou vrstvou obvykle korespondují s řešením algoritmů pro dynamické přidělování šířky pásma pro sítě s prodlouženým dosahem. Například [81] prezentuje vlastní algoritmy pro dynamické přidělení šířky pro sítě s prodlouženým dosahem. Oba algoritmy jsou schopné prodloužit dosah distribuční sítě až na 100 km. Zvýšením dosahu distribuční sítě vyvstává důležitý faktor, a to zachování útlumových tříd a časování jednotek, neboť bez úpravy přenosové vrstvy nelze obsloužit všechny jednotky. Autoři [82] se zabývali uvedeným nedostatkem. Hlavní nevýhodou je nutnost FPGA polí pro danou OLT jednotku. Uvedené řešení nebude pravděpodobně masově nasazováno, neboť hlavním nedostatkem řešení je cena. Výhodou řešení je potom prodloužení dosahu distribuční sítě na 60 km a zachování časových slotů v rovnoměrném rozložení pro všechny jednotky (až do 512 ONU). Článek [83] navrhuje změnit přístupovou GPON síť na metropolitní síť založenou na sítích další generace za použití prodlouženého dosahu do 100 km a úpravou přenosové vrstvy. V rámci komunikace v EPON sítích je využíván registrační protokol pro koncové jednotky, který je zcela odlišný od GPON sítí. Článek [84] poskytuje analýzu stability a zpoždění pro tento protokol za pomocí Markovových řetězců v rámci simulačního modelu EPON sítě.

Další publikace [85] poskytuje rozdílný pohled na PON sítě, a to z hlediska kombinace různých datových zdrojů (Ethernet, byznys služby, node B a GPON data) a jejich slučování do 10Gbit toku. Hlavním nedostatkem zůstává problematika mapování různých datových toků do výsledné PON sítě, protože každá síť, založena na ITU, využívá jiný formát rámce. Další možností pro prodloužení dosahu sítě může být využití aktivního zesilovače. Tuto možnost zvažují v [86] za pomocí Ramanovského zesilovače. Vzhledem k tomu, že již jsou dostupné metody pro prodloužení dosahu distribuční sítě i bez zesilovačů, není zcela nezbytné jeho využití. Nehledě na to, že nezůstává zachována pasivita sítě. Významným článkem v této oblasti je [87]. Článek se zabývá oznamováním a plánováním vzestupného směru pro 1/10G EPON a GPON sítě. Sestupný směr je přenášen všesměrově, proto se tímto směrem autoři nezabývali. Vzestupný směr v EPON a GPON je založen na rozdílných metodách. Obecně nelze obě tyto sítě porovnat, protože GPON není založen na přístupové metodě CSMA (Carrier Sense Multiple Access – metoda mnohonásobného přístupu k médiu). GPON sítě zachovávají rovnoměrné rozdělení časových slotů pro koncové jednotky, avšak z IP síti je charakteristická kvalita služby QoS (Quality of Service – kvalita služby) [88]. Prezentované řešení se opírá o dynamické váhování front a prioritizování vybraného provozu za pomocí REPORT zpráv. Porovnání kapacity linky a její zpoždění pro sítě EPON, GPON a NG-PON poskytuje [89].

Jak již bylo několikrát zmíněno standardy podle IEEE a ITU jsou zcela odlišné a nejsou vzájemně kompatibilní. Z tohoto důvodu je věnována velká pozornost ekonomické stránce obou řešení [90], [91] a [92].

4.4.2 Princip navázání spojení

Princip navázání spojení vychází ze základní topologie GPON standardu. Podle základní topologie zobrazené na obr. 4.5 je zřejmé, že jednotky ONU od sebe nemohou být stejně vzdálené. Každý zákazník bydlí v jiném patře, má jinak situován byt atd., proto je stejná délka (s přesností na metry) vyloučena. Tento předpoklad hraje významnou roli během sestavení zpoždění a přidělování tzv. ekvalizačního zpoždění, které má za úkol dorovnávat délky vláken mezi jednotlivými zákazníky. Bude-li délka vyrovnána pomocí ekvalizačního zpoždění, dojde zároveň k vyrovnání rychlosti šíření signálu, tedy bude zajištěno přesné přidělování časových slotů.

Počáteční inicializace probíhá ihned po připojení nové ONU jednotky (připojení nového zákazníka) do sítě poskytovatele služeb. V oblasti počítačových sítí by došlo k oznámení nové připojené stanice na základě MAC (Media Access Control – identifikátor síťového zařízení) adresy, optické sítě tyto adresy nevyužívají, proto musí řídicí jednotka OLT pravidelně odesílat synchronizační rámce. Doba trvání tohoto rámce je 125 µs a obsahuje tzv. PSBd (Physical Synchronization Block downstream – synchronizační blok v sestupném směru) hlavičku spolu se synchronizačním polem PSync (Physical Synchronization – synchronizace sestupného směru). Nově připojená koncová jednotka ONU musí projít celkem pěti stavy, aby byla schopna komunikovat v síti poskytovatele služeb. Výchozím stavem je tzv. inicializační stav (O1). Do tohoto stavu se koncová jednotka dostane přijetím minimálně 2 synchronizačních rámců, ve kterých je porovnávaná hodnota obsažena v Psync části s fixním obsahem $0\times B6AB31E0$. Standard [53] udává, že minimální shoda z Psync části je stanovena na 62 ze 64 bitů, jedná se pouze o doporučení, které závisí na implementaci jednotlivých výrobců [53]. Inicializační stav lze dále rozdělit na tři další podstavy, tzv. hunt stav, v rámci něj dochází pouze k příjmu rámců od OLT a dochází ke hledání Psync části. Koncová jednotka ONU automaticky nastaví parametry LOS (Loss of Signal – ztráta signálu)/LOF (Loss of Frame – ztráta rámce) na hodnotu 1. Po nalezení Psync části a dekódování prvního rámce jednotka přechází do před-synchronizačního stavu a očekává přijetí dalšího rámce s Psync částí. Počet úspěšných shod v rámcích je stanoven výrobcem a neexistuje obecná hodnota. Teprve po přijetí M synchronizačních rámců jednotka přejde do posledního ze tří stavů, tedy synchronizačního stavu. Jinými slovy se jednotka přesune do stavu Standby (O2) a dojde ke změně hodnot LOS/LOF na 0.

Ve stavu O2 má ONU jednotka synchronizován pouze sestupný směr (od OLT k ONU), přesto stále není schopná přijímat datové rámce v tomto směru. Jednotka ONU nyní očekává přijetí zprávy $Upstream\_Overhead\_PLOAM$. Zpráva je šířena ve směru od OLT k ONU, a to celkem 3×, jejíž obsahem jsou parametry sítě (hodnota oddělovače pro rámce, výkonová úroveň a před-přidělené zpoždění pro eliminaci

vzdálenosti). Nastavením parametrů může ONU přejít do Serial Number stavu (O3). Zároveň OLT jednotka po odeslání tří zpráv *Upstream_Overhead_PLOAM* musí vyčkat 750 µs [11], aby ONU jednotka měla čas na zpracování.

Ani ve stavu O3 není jednotka ONU stále schopna komunikovat s OLT jednotkou pomocí datových rámců ani dekódovat příchozí datové rámce. Zároveň ve stavu O3 vstupuje do komunikačního schématu časovač TO1, nastavený na hodnoty 10 s. Koncová jednotka ONU očekává přijetí zprávy *AssignONU-ID* od OLT jednotky. Mezitím OLT jednotka vytvoří tzv. tiché okno o délce 250 µs pomocí zprávy *BWmap*. Přijetím zprávy *BWmap* všech koncových jednotek na síti, dojde k přerušení vysílání, aby nedošlo ke kolizi. Po dobu trvání tichého okna OLT odešle další rámec, který obsahuje v PLOAM části zprávu *Serial_Number_Request* adresovanou na *Alloc-ID* $0\times FE$ (tato hodnota je předurčena pro aktivační proces) s 13B grantem a *StartTime* 77 µs. Po zpracování zpráv a nastavení parametrů ONU čeká náhodný čas (z intervalu 0–48 µs) spolu s připočtením hodnoty 77 µs (*StartTime* hodnota), jakmile uplyne nastavený čas, ONU jednotka odešle zprávu *Serial_Number_ONU*, v níž je oznámeno vygenerované zpoždění (z intervalu 0–48 µs) jednotce OLT. Zprávě *Serial_Number_ONU* předchází hlavička PLOu (Physical Layer oVERHEAD UPSTREAM – synchronizační část zprávy ve vzestupném směru) z důvodu synchronizace. Po přijetí zprávy *Serial_Number_ONU* OLT jednotkou je nezbytné vyčkat a přijmout i zbylé dvě zprávy (zpráva je šířená celkem 3×), na které OLT jednotka reaguje odesláním zprávy *Assign-ID* s unikátním sériovým číslem. Sériové číslo odesílané ve zprávě *Serial_Number_ONU* je částečně tvořeno výrobním číslem jednotky a náhodně vygenerovanými údaji. *Assign_ONU-ID* nastavuje klíčový parametr *ONU-ID* pro přímé adresování jednotek (je tedy pro každou jednotku unikátní) a jeho přijetí musí proběhnout před uplynutím časovače TO1 (10 s). V reálné síti časovač TO1 vyprší, pokud se připojuje více než 10 ONU jednotek ve stejném čase, protože přiřazení *Assign_ONU-ID* probíhá recipročně. Koncová jednotka ONU pro přijetí *Assign_ONU-ID* přechází do stavu Ranging (O4).

Na začátku této podkapitoly byla popsána funkce ekvalizačního zpoždění. Toto zpoždění je nastavováno během stavu O4 za účelem eliminování rozdílných délek vláken ke koncovým jednotkám. Výpočet ekvalizačního zpoždění provádí OLT jednotka pomocí následujícího vztahu [53]:

$$\begin{aligned} Teqd &= T_{1490,i} + RspTime_i + EqD_i + T_{1310,i} = \\ &= T_{1490,i}\frac{n_{1310}+n_{1490}}{n_{1490}} + RspTime_i + EqD_i, \end{aligned} \tag{4.1}$$

kde: $RspTime_i$ odpovídá době odpovědi (µs), EqD odhad ekvalizačního zpož-

[11] Hodnota je stanovena standardem [53], ale výrobci zařízení ji mohou libovolně měnit.

dění pro délku vlákna na základě prvního vztahu, n_{1310} index lomu pro $\lambda = 1\,310\,\text{nm}$ v distribuční síti, n_{1490} index lomu pro $\lambda = 1\,490\,\text{nm}$ v distribuční síti. Zlomek se skupinovou rychlostí může být upraven následovně [53]:

$$T_{1490,i} = (Teqd - RspTime_i - EqD_i)\frac{n_{1490}}{n_{1310} + n_{1490}}, \tag{4.2}$$

Substitucí výrazu pro přijetí n-tého GTC rámce vztah dostane podobu [53]:

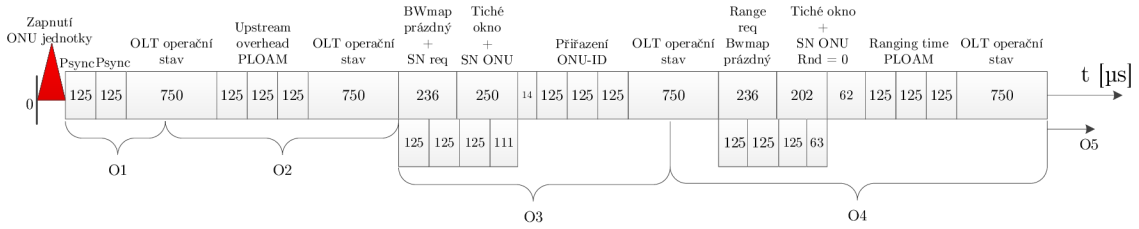
$$Trecv_{N,i} = Tsend_{N,i} + T_{1490,i}. \tag{4.3}$$

Kompletní vztah pak bude vypadat následovně [53]:

$$\begin{aligned} Trecv_{N,i} = Tsend_N + Teqd\left[\frac{n_{1490}}{n_{1310}+n_{1490}}\right]_{OLT} \\ -(EqD_i + RspTime_i)\left[\frac{n_{1490}}{n_{1310}+n_{1490}}\right]_{ONU}. \end{aligned} \tag{4.4}$$

Přijetím hodnoty ekvalizačního zpoždění ONU jednotka přechází do stavu Operation (O5). V rámci navázání spojení je stav Operation konečný, tedy jednotka ONU je schopná jak vysílat, tak i přijímat datové rámce od OLT jednotky.

Výše uvedený popis lze shrnout pomocí obr. 4.12.



Obr. 4.12: Detaily přenášených zpráv a tichých oken během sestavení spojení mezi OLT a ONU

4.4.3 Simulace navázání spojení

Experimentální nastavení simulačního nástroje Matlab vychází z definic několika parametrů. První $nONU$ představuje počet ONU jednotek, které se chtějí připojit do sítě a nabývá hodnot 2, 4, 8, 16, 32, 64 a volitelně 128. Definované hodnoty udávají dělicí poměr 1:x, kde x je nahrazeno dříve uvedenými hodnotami. Poslední zmíněná 128 je pouze volitelná, neboť standard s takto vysokým dělicím poměrem nepočítá[12]. Konstanta fd předává hodnotu 125 µs, což odpovídá době trvání rámce. Časovač $TO1$ je nastaven na 10 s. Proměnná $curTime$ je použita jako čítač reálného času

[12]V prvním svém návrhu. Druhá přepracovaná verze tento dělicí poměr povoluje.

a je nastavena na 0 a po uplynutí časovače $TO1$ oznámí proměnnou *delay* přetečení, když *curTime* přesáhne hodnotu $TO1$. Obdobně proměnná ONU uchovává pole třídy ONU s hodnotou vzdálenosti a ekvalizačním zpožděním. Posloupnost rámců z obr. 4.12 se v rámci simulací opakuje každou sekundu. Pro dosažení shody s Initial stavem je hodnota M_1 nastavena na 2, proto je nezbytné, aby ONU jednotka přijala minimálně 2 synchronizační rámce.

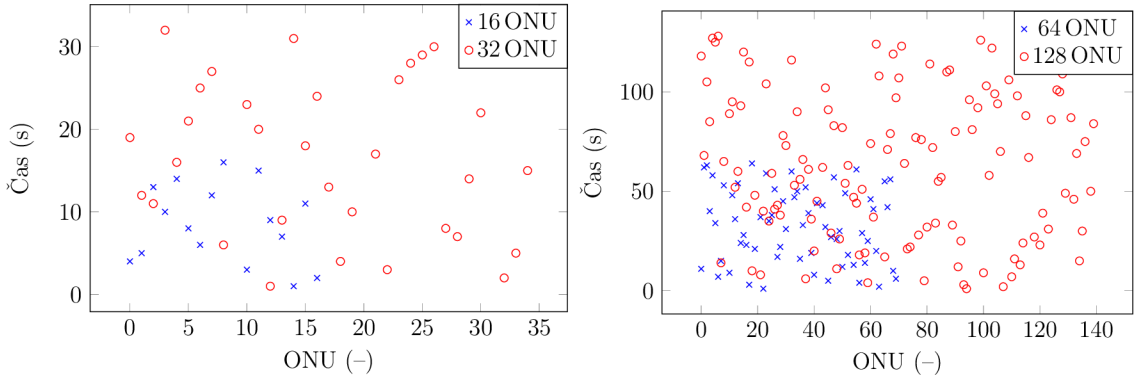
Před započetím simulací je nutné nastavit rozsah vzdáleností ONU jednotek od OLT jednotky. V případě reálných sítí je nejvyšší možná vzdálenost stanovena na 20 km. Z tohoto důvodu byl zvolen rozsah 0–20 km, kde aplikace sama vygeneruje odpovídající počet vzdáleností (podle proměnné $nONU$). Druhý krok simulace tvoří výpočet propagačního zpoždění a přidání náhodného zpoždění z rozsahu 0–48 µs pro každou ONU jednotku. OLT jednotka udržuje zprávu $Serial\_NumberONU$ od všech ONU jednotek. Ze všech příchozích zpráv $Serial\_NumberONU$ OLT jednotka vybere první (doručenou první v čase) a této jednotce odpoví zprávou $AssignONU\text{-}ID$. Ostatní ONU jednotky musí čekat, než dojde k přijetí zprávy $AssignONU\text{-}ID$ s jejich sériovým číslem. Výše uvedený princip se periodicky opakuje každou 1 s. Na tuto hodnotu je nastavena i proměnná $curTime$. V každém průchodu programu je hodnota $curTime$ porovnána s hodnotou časovače $TO1$. Jakmile dojde k přetečení $curTime$ proměnné, všechny ONU jednotky, které neobdržely zprávu $AssignONU\text{-}ID$ s jejich sériovým číslem, přechází zpět do Standby stavu (O2) a hodnota *delay* bude navýšena o 1, neboť další zpráva $AssignONU\text{-}ID$ nebyla přijata. Vztah pro výpočet simulací je dán rovnicí:

$$t_a = \left(\left(35 + 2 \cdot \left(ceil\left(\frac{MRTD + QW}{fd}\right)\right)\right) \cdot fd\right) + delay + (i\ -1)\,, \tag{4.5}$$

kde: 35 udává minimální počet rámců pro navázání spojení dle [53], funkce *ceil* v Matlabu zaokrouhluje desetinná čísla na celá čísla, $MRTD$ uvádí maximální round trip zpoždění, QW tzv. tiché okno (250 µs), fd je doba trvání rámce (125 µs), *delay* odpovídá době šíření pro jednotlivé ONU podle jejich vzdáleností a i je čítač cyklů.

Simulace byly rozděleny do dvou scénářů. První se zabýval porovnáním doby připojení 16 a 32 ONU jednotek a druhý porovnával čas pro 64 a 128 ONU jednotek. Výsledky obou scénářů zobrazuje obr. 4.13.

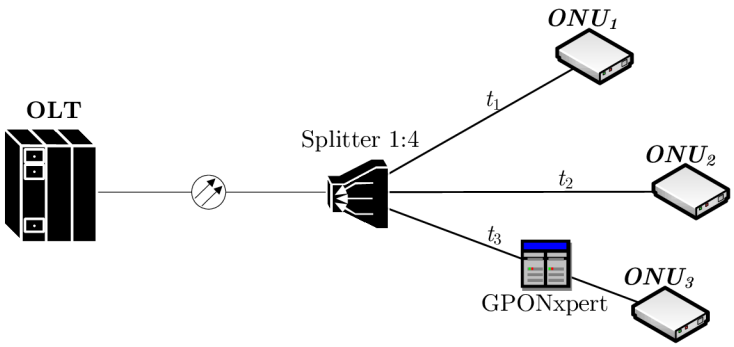
Podle dosažených výsledků z obr. 4.13 pro připojování ONU vyplývá, že nízký počet jednotek je centrální jednotka schopna obsloužit v nízkém čase (pro nastavení $TO1$ 10 s). Celkový počet 32 zákazníků je v prvotní fázi připojeno do 32 s. Při vyšším počtu ONU je znát prodleva mezi jednotlivými stavy a pro poslední ONU jednotku z 64 přítomných je doba přípojení ≈75 s. Tato hodnota je dána vypršením časovače $TO1$ a inkrementací *delay*, která je vždy navýšena po uplynutí časovače $TO1$.



Obr. 4.13: Vlevo: Doba připojení 16 a 32 ONU jednotek do sítě poskytovatele. Vpravo: Doba připojení 64 a 128 ONU jednotek do sítě poskytovatele.

4.4.4 Měření experimentální GPON sítě

Ověření výsledků pomocí měření probíhalo na experimentální síti GPON. Topologie sítě je zobrazena na obr. 4.14, jediným rozdílem mezi obr. 4.5 byl rozbočovač s dělicím poměrem 1:4.



Obr. 4.14: Topologie GPON experimentální sítě analyzované GPONxpertem

Před zvolenou jednotku byl umístěn měřicí přístroj GPONxpert[13]. Zařízení GPONxpert je v České republice ojedinělé zařízení, kterým disponují pouze velcí operátoři. Většina dostupných měřicích přístrojů zpracovává parametry fyzické vrstvy, je-li nezbytné zpracovávat zprávy na vyšších vrstvách, musí být použito GPONxpertu. I měření bylo rozděleno na dva scénáře. První scénář měřil přenos zpráv při deaktivaci ONU jednotky v rámci sítě poskytovatele služeb. ONU, jenž má být deaktivováno odesílá tři zprávy: *Remote Error Indication*, *Dying Gasp* a *Deactivate ONU-ID* (viz tab. 4.4).

[13]Měření probíhalo v síti Orange SK. Touto cestou bych rád společnosti poděkoval, zejména Ing. Luboši Dubravci za ochotu a pomoc s měřením.

Tab. 4.4: Zprávy zasílané ONU jednotkou při odhlášení ze sítě

Čas	**ONU-ID**	**Typ zprávy**	**Zdroj zprávy**	**Směr**
00:00:04.364	1	Remote Error Indication	PLOAM zpráva	↑
00:00:09.364	1	Remote Error Indication	PLOAM zpráva	↑
00:00:14.365	1	Remote Error Indication	PLOAM zpráva	↑
00:00:19.365	1	Remote Error Indication	PLOAM zpráva	↑
00:00:24.364	1	Remote Error Indication	PLOAM zpráva	↑
00:00:29.364	1	Remote Error Indication	PLOAM zpráva	↑
00:00:31.933	1	Dying Gasp	PLOAM zpráva	↑
00:00:31.934	1	Dying Gasp	PLOAM zpráva	↑
00:00:31.935	1	Dying Gasp	PLOAM zpráva	↑
00:00:36.079	1	Deactivate ONU-ID	PLOAM zpráva	↓
00:00:36.080	1	Deactivate ONU-ID	PLOAM zpráva	↓
00:00:36.080	1	Deactivate ONU-ID	PLOAM zpráva	↓

Z tab. 4.4 je patrné, že ONU jednotka zasílá zprávu *Remote Error Indication*, jenž ve svém těle obsahuje indikátor ztráty signálu a rámců. Přibližně po 30 s ONU jednotka odesílá zprávu *Dying Gasp*, čímž dojde k oznámení vypnutí této jednotky. Na tyto zprávy reaguje OLT jednotka zprávou *Deactivate ONU-ID*. Teprve po přijetí těchto tří zpráv je ONU jednotka kompletně odhlášena ze sítě.

Druhý scénář pokrýval analýzu přenášených zpráv odesílaných mezi jednotkou OLT a ONU během aktivačního procesu. Byť bylo možné přístrojem GPONxpert vyhodnotit přenášené zprávy v rámci komunikace, byl objeven drobný nedostatek a to, že časové údaje jsou přenášeny v ms místo µs. Posloupnost zpráv zachycených během komunikace mezi OLT a ONU_3 zobrazuje tab. 4.5.

Uvedená tabulka zobrazuje první zprávu *Assign ONU-ID*, tato zpráva však netvoří počátek celého procesu. Měřicí přístroj GPONxpert není schopen detekovat synchronizační rámce a zprávu *Upstream Overhead*, kterou OLT jednotka pravidelně vysílá. Samotný simulační model pokrývá veškeré zprávy, které jsou přenášeny během aktivace podle obr. 4.12. Poslední uvedená zpráva zobrazuje přítomnost zabezpečení, výměna klíčů probíhá nad stavem Ranging (O4) a jedná se o volitelnou část, která je ve výchozí konfiguraci vypnuta (nastavena na 0). Při sečtení všech časů v navrženém schématu podle obr. 4.12 a výsledků z měření tab. 4.5 dojde k dosažení stejných hodnot připojování jednotek.

Výsledky měření a simulace spojení byly publikovány v [93].

Tab. 4.5: Zprávy z aktivačního procesu jednotky ONU_3

Čas	ONU-ID	Typ zprávy	Zdroj zprávy	Směr
00:01:41.508	Broadcast	Assign ONU-ID	PLOAM Message	↓
00:01:41.508	Broadcast	Assign ONU-ID	PLOAM Message	↓
00:01:41.508	Broadcast	Assign ONU-ID	PLOAM Message	↓
00:01:41.620	1	Ranging Request	BWmap Event	↓
00:01:41.621	1	Serial number ONU	PLOAM Message	↑
00:01:41.731	1	Ranging Request	BWmap Event	↓
00:01:41.731	1	Serial number ONU	PLOAM Message	↑
00:01:41.827	1	Ranging Time	PLOAM Message	↓
00:01:41.827	1	Ranging Time	PLOAM Message	↓
00:01:41.827	1	Ranging Time	PLOAM Message	↓
00:01:41.937	1	Request password	PLOAM Message	↓

4.4.5 Nový algoritmus připojování jednotek

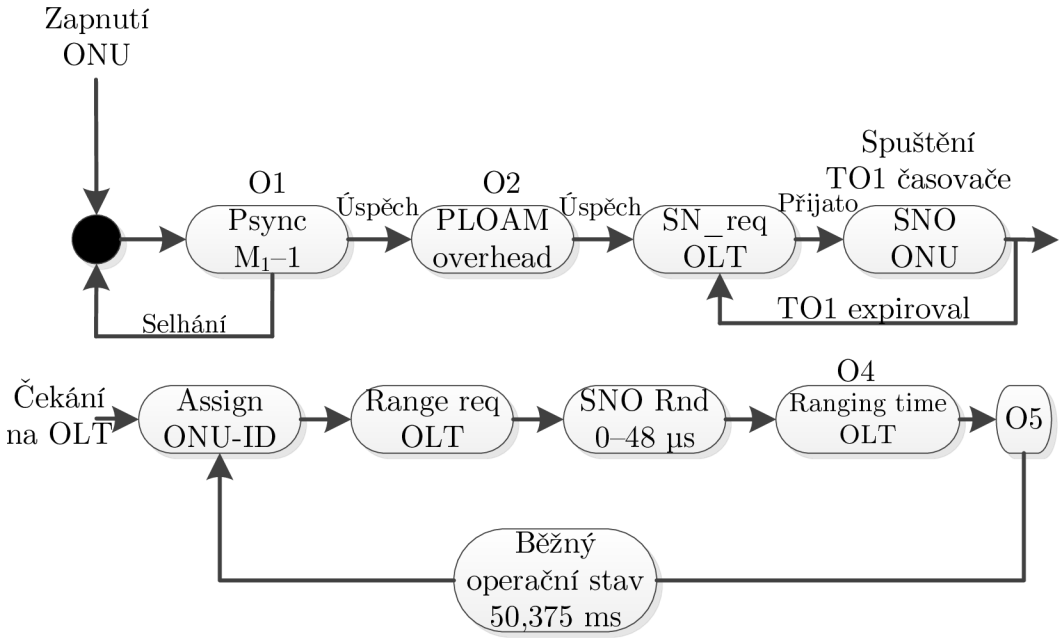
Základem nového algoritmu je zkrácení doby aktivačního procesu pro koncové jednotky. Zpočátku simulačního modelu[14] je vygenerováno pole o obsahu n-ONU jednotek v náhodné vzdálenosti od OLT do 20 km. Následně je pole seřazeno vzestupně z pohledu vzdálenosti ONU (seřazení koncových jednotek je klíčové pro dosažení odpovědí od první jednotky, která bude v nejkratší vzdálenosti a OLT vybere danou ONU a odešle první Assign ONU-ID zprávu). Následně dochází k odstartování smyčky pro všechny ONU jednotky, která počítá hodnoty zpoždění pro všechny ONU připojené do simulované sítě. Pro první ONU lze algoritmus charakterizovat za pomocí následujících proměnných:

- $21 \times f_d$ – kde se ONU synchronizuje ve vzestupném směru za použití přijímání Upstream Overhead PLOAM pro nastavení síťových parametrů a odpovídá zprávou Serial Number ONU.
- $16 \times f_d$ – zde probíhá přiřazení ONU-ID, odpovídá se na zprávu Ranging Request zprávou Serial Number ONU a přijetím zprávy Ranging Time upravuje hodnotu ekvalizačního zpoždění dané jednotky[15].
- $3 \times f_d$ – ONU vstoupí do operačního stavu O5. Tato fáze je i volitelná, není nezbytná, umožňuje pouze OLT jednotce informovat danou ONU o připravenosti obousměrné komunikace.

[14] Vytvořeného v Matlabu.
[15] Závislé na vzdálenosti od OLT.

Celkový čas pro připojení ONU jednotky je dán $40 \times f_d$ (5 ms). Následně OLT odešle další Assign ONU-ID zprávu každých 403 rámců (50,375 ms) pro připojení druhé nejbližší ONU, tedy druhá jednotka bude aktivována po $403 \times f_d + 3 \times f_d$ (52,750 ms). Celý proces je zopakován 19×. Po tuto dobu je OLT jednotka schopna připojit celkově 20 ONU v 1 s. Nutno poznamenat, že se zde nachází 2rámcová mezera mezi poslední ONU v cyklu a první ONU v dalším druhém cyklu, proto je připojení ONU zpočátku opožděno o 250 µs. Maximální limit dosavadních GPON sítí je 128 ONU jednotek na jeden port OLT [53]. Aktivace limitního počtu ONU lze dosáhnout ≈7 s.

Poskytovatelé služeb v dnešních sítích stále používají aktivační proces, jenž je definován [53], nicméně výrobci mohou provést změny (za použití nespecifikovaných polí v PLOAM zprávách). Jedná se pouze o doporučení, které zajišťuje zpětnou kompatibilitu mezi výrobci. Navržený algoritmus může být nezávisle implementován, díky použití stávajících zpráv ve stejném formátu a typu. Detaily algoritmu jsou zobrazeny na obr. 4.15. Inicializační fáze je shodná s běžným algoritmem. Hlavní nevýhodou je malé množství aktivovaných jednotek ve stejném čase. Některé parametry: předdefinované zpoždění (preassigned delay) a ONU-ID jsou přenášeny všesměrově. Nicméně koncové ONU jednotky porovnávají vlastní sériové číslo nebo ONU-ID pro zpracování vlastních dat. Během všesměrového přenosu může OLT zpracovávat data nejméně po dobu 750 µs, a to zejména při přenosu Upstream Overhead a Assigned ONU-ID PLOAM zpráv.



Obr. 4.15: Detaily navrženého algoritmu pro GPON sítě

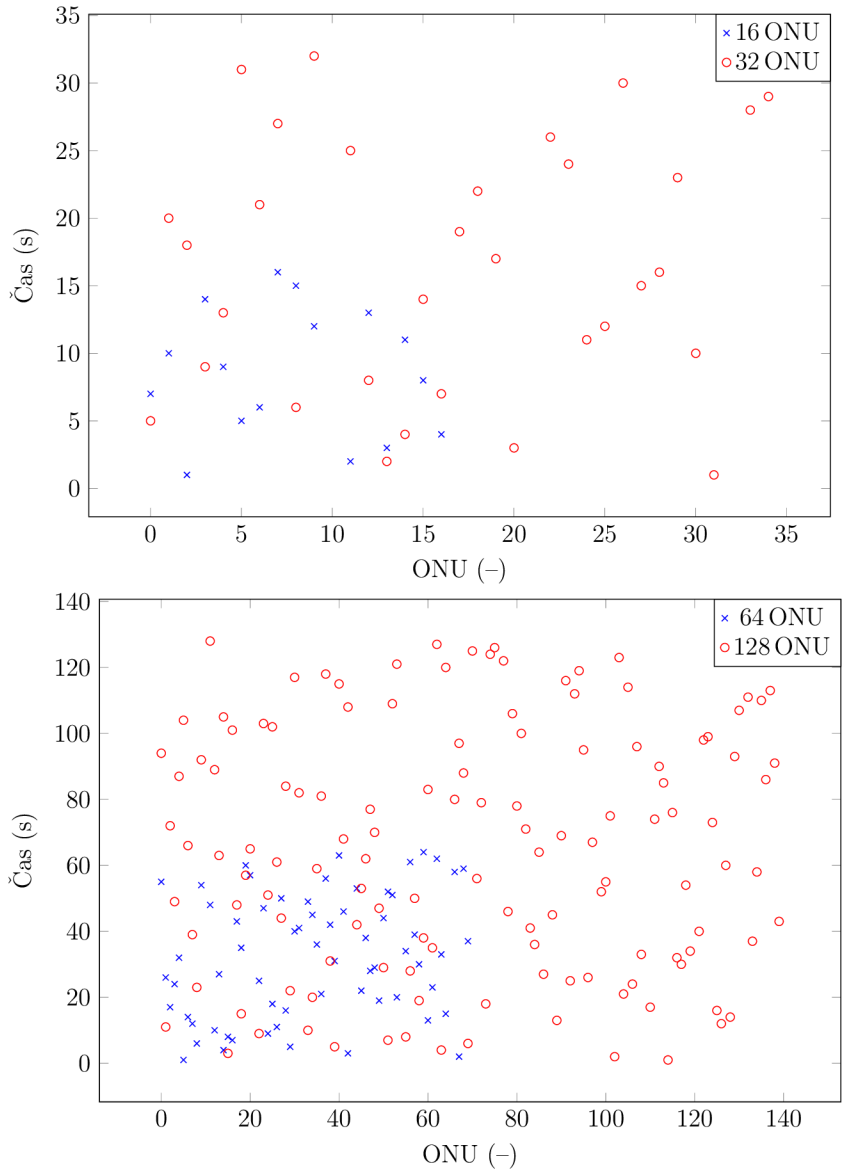
V rámci navrženého algoritmu byla zachována doba 750 µs před odesláním další PLOAM zprávy. Na druhou stranu výrobci systémů mohou tuto hodnotu libovolně měnit (navyšovat), čímž by bylo zapříčiněno prodloužení aktivační doby jednotek. Rovněž je předpokládáno přenosu stejných parametrů za použití více grantů pro ONU. Hlavním cílem je urychlení aktivačního procesu po rozsáhlém výpadku dodávky elektrické energie (blackout), neboť po obnovení dodávky energie bude vyžadována opětovná registrace k OLT. Určitou dobu (v závislosti na zvoleném aktivačním procesu) nemohou zákazníci využívat předplacené služby do opětovné aktivace ONU. Kupříkladu, bude-li bráno v potaz 1024 ONU jednotek, pak jsou nezbytné desítky minut nebo hodiny pro znovuobnovení registrace všech jednotek. Díky navrženému algoritmu by bylo možné dosáhnout opětovné aktivace 1024 ONU řádově v jednotkách minut.

Simulační model byl rozdělen do dvou scénářů (stávající a nový algoritmus). Výsledky simulací byly uspořádány podle dělicího poměru se stejným algoritmem. Obecně je uvažována TC vrstva pro ONU a OLT, optická vlákna (rychlosti šíření a indexem lomu) a jejich délkou od 1–20 km. Výsledky simulací pro 16 a 32 ONU jednotek se stávajícím algoritmem jsou zobrazeny na obr. 4.16 nahoře, nebyla tedy provedena žádná úprava stavového automatu ani formátu zpráv.

Obecně současný algoritmus umožňuje připojit pouze jedinou ONU během jednoho průchodu. V nejhorším případě (blackout) bude poslední jednotka připojena za 33 s. Na druhou stranu reálná síť nikdy nebude obsahovat takto nízký počet koncových jednotek. Druhý simulační scénář se zabýval simulacemi pro 64/128 ONU, výsledky jsou zobrazeny na obr. 4.16 nahoře. Druhý scénář dosáhl vyšších hodnot. Pokud by bylo uvažováno standardní OLT se 4, 8 nebo 16 porty pro splittery a ODN, což znamená 8× větší konečný čas pro připojení jednotek (uvažováno pro OLT s jedním CPU). Jinými slovy výsledky by musely být vynásobeny počtem portů na OLT. V nejlepším případě bude poslední jednotka připojená po 500 s v nejhorším případě po 2000 s. Z těchto důvodů byla navržena optimalizace stávajícího algoritmu s dodržením formátu rámce a typů zpráv.

Díky nově navrženému algoritmu bylo dosaženo ≈7× nižší doby připojení poslední jednotky v porovnání s běžným algoritmem. Poslední ONU jednotka bude připojena, v simulačním scénáři pro 32 ONU, za ≈2 s při zachování formátu PLOAM zpráv. Není vyžadován žádný specializovaný HW, neboť došlo k modifikaci tzv. tichého okna. OLT jednotka využívá tiché okno pro zpracování odpovědí od ONU jednotek a k přípravě dalších zpráv. Druhý scénář s vyšším dělicím poměrem (1:64/128) podává zajímavější výsledky.

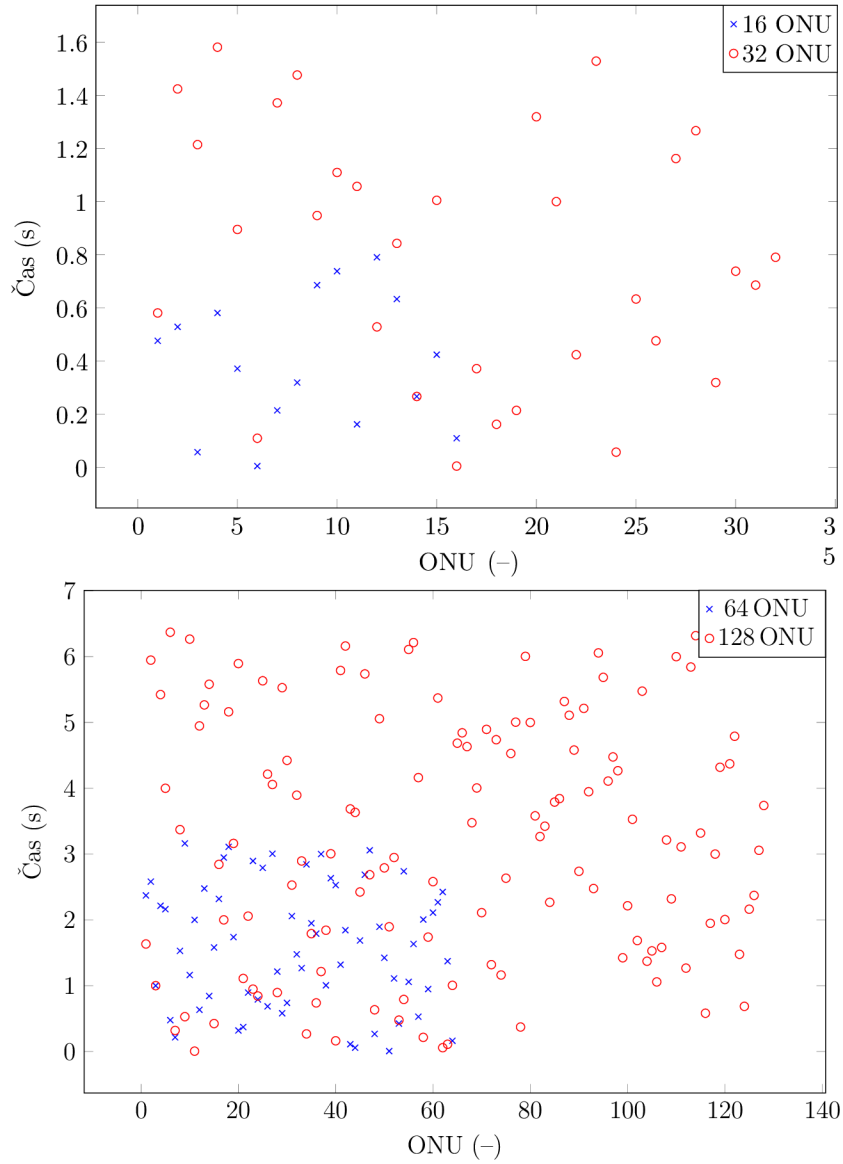
Poslední simulace aktivačního procesu jsou zobrazeny na obr. 4.17 dole. Čas ≈7 s pro poslední ONU vychází z obr. 4.17. V nejhorším případě, při uvažování OLT se čtyřmi porty (každý z nich bude obsluhovat 128 ONU jednotek), bude dosaženo



Obr. 4.16: Nahoře: Doba připojení 16 a 32 ONU jednotek podle [53] Dole: Doba připojení 64 a 128 ONU jednotek podle [53]

≈28 s pro jeden port a ≈112 s pro 4 porty. V porovnání se stávajícím algoritmem bylo dosaženo (v nejlepším případě) 9× nižšího celkového času připojení. Kupříkladu, dojde-li k poškození OLT, s navrženým algoritmem budou koncoví zákazníci bez služeb pouze na nezbytně krátkou dobu v porovnání se stávajícím algoritmem.

Výše popsané výsledky byly publikovány v [94].



Obr. 4.17: Nahoře: Doba připojení 16 a 32 ONU jednotek po optimalizaci Dole: Doba připojení 64 a 128 ONU jednotek po optimalizaci

4.5 Princip komunikace v GPON sítích

GPON sítě umožňují přenášet data oběma směry, avšak mezi těmito směry je zásadní rozdíl v podobě přenosu. Sestupný směr (od OLT k ONU) je centralizován do OLT jednotky, která poskytuje data, zapouzdření, formátování rámce aj. pro každou ONU. Jak již bylo zmíněno, distribuční síť obsahuje pouze pasivní prvky, čímž je docíleno pasivního rozbočení sestupného směru všem ONU jednotkám. Oproti tomu vzestupný směr je distribuován v unicastové komunikaci, protože se předpokládá, že každá ONU jednotka bude mít rozdílná data.

4.5.1 Komunikace v sestupném směru

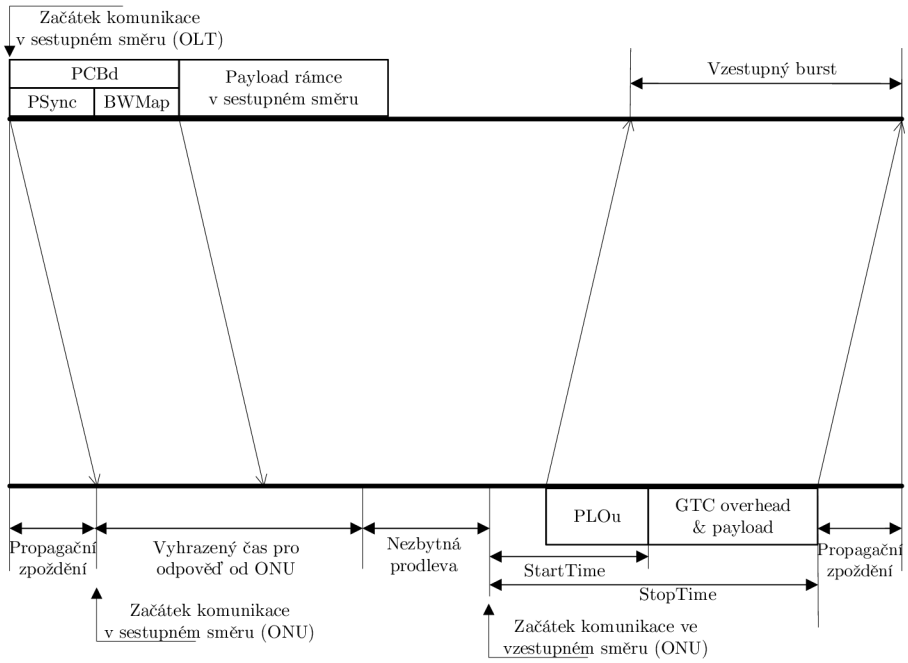
Sestupný směr je centralizován do OLT. OLT multiplexuje GEM rámce do přenosového média za použití GEM Port-ID. Identifikátor Port-ID odděluje koncové jednotky ONU, což znamená, že jeden rámec může obsahovat data pro více koncových ONU. Obecně si lze tyto identifikátory představit jako logické spojení mezi OLT a ONU, která jsou oddělená. Z tohoto důvodu využívá sestupný směr všesměrového vysílání, tedy každá jednotka přijme veškerá data, ačkoli jsou zpracovány rámce pouze s odpovídající Port-ID, ostatní jsou zahazovány.

4.5.2 Komunikace ve vzestupném směru

Komunikace ve vzestupném směru využívá jiného principu. Obecně OLT jednotka odesílá rámce pro ONU s přesně určenými parametry nebo tzv. vzestupnou alokací šířky pásma pro odpovídající vztah s nutnou hodnotou dat, která jsou připravena pro odeslání[16][53]. Daná hodnota požadavku je identifikována vlastními Alloc-ID. Alokační identifikátor je 12bit číslo, jenž přiřazuje OLT. V terminologii GPON sítí by bylo možné označit hodnotu požadavku pro alokaci šířky pásma jako T-CONT (Transmission Container – přenosový kontejner dat v GPON sítích) nebo OMCC (Optical Network Unit Management and Control Channel – řídicí a kontrolní kanál v GPON sítích). Počet Alloc-ID je vždy vymezen minimálně na jeden, který odpovídá hodnotě ONU-ID (obdoba unikátní hardwarové adresy) a je platná po celou dobu zapnutí ONU. Z charakteru PON sítě je zřejmé, že každý zákazník se bude nacházet v rozdílné vzdálenosti od OLT, čímž budou vyžadovány jiné parametry zpoždění. Modelový případ komunikace zobrazuje obr. 4.18.

Nejdříve OLT připraví rámec s následujícími parametry: PCBd (Physical Control Block downstream – synchronizační blok fyzické vrstvy), PSync, BWmap (Bandwidth Map – informace o počtu přidělených časových slotů pro ONU) a payload rámce v sestupném směru (data). PCBd je pouze kontrolní část sestupného směru daného rámce, PSync je synchronizační část, aby bylo docíleno synchronizace mezi OLT a ONU (více v kapitole 4.4.2), BWmap reprezentuje hodnotu (zpravidla dobu) komunikace ve vzestupném směru dané ONU. Rámec se všemi parametry je přenášen distribuční sítí pro všechny ONU (v různých vzdálenostech). Jakmile ONU přijme hlavičku PCBd s PSync a zná čas přijetí. Nejdůležitějším parametrem z pohledu komunikace je BWmap, protože specifikuje, kdy a kolik dat může být odesláno k OLT, neboť ONU má pouze omezený čas pro přípravu rámce na odpověď ($35 \pm 1\,\mu s$). Na obr. 4.18 je dále zobrazena hodnota, nezbytné zpoždění, která má za

[16] V principu zjišťováno dynamickými algoritmy pro přidělení šířky pásma.



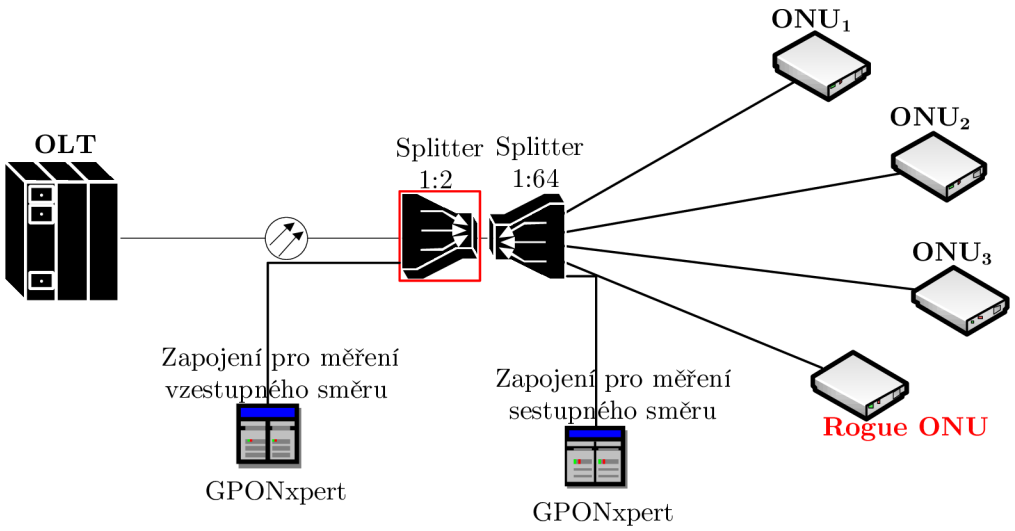
Obr. 4.18: Časová návaznost pro komunikaci ve vzestupné směru

úkol eliminovat rozdílné vzdálenosti mezi ONU a OLT, odlišné doby zpracování dílčích ONU a zabránit kolizím v komunikaci na přenosovém médiu. Nezbytné zpoždění koresponduje s ekvalizačním zpožděním specifikovaným OLT během Ranging stavu (viz kapitola 4.4.2).

4.5.3 Měření v síti Orange SK

Předchozí podkapitoly popisovaly princip komunikace v obou směrech. Základním principem vzestupné komunikace je rozdělit dostupnou šířku pásma za použití časových slotů a jednotlivé sloty adekvátně rozdělit mezi koncové jednotky ONU díky identifikátoru BWmap. Z tohoto důvodu nelze měřit pouze na jednom výstupním portu splitteru, neboť by nebyly zachyceny všechny upstream shluky (bursty). Proto je nezbytné přidat další splitter pro vydělení veškeré vzestupné komunikace. Rovněž je nezbytné počítat s prodlevou v analýze, neboť GPONxpert není schopen poskytnou analýzu v reálném čase[17]. Pro ukládání dat a jejich následné zpracování je použito FPGA polí. Níže uvedený obr. 4.19 zobrazuje zapojení pro měření obou směrů (postupné měření). Dodatečný splitter (na obr. 4.19 zvýrazněn červenou barvou) disponoval dělicím poměrem 1:2 (z důvodu zachování útlumové bilance sítě). Běžně se ponechává rezerva v distribuční síti cca 3 dB.

[17]Pro tuto možnost je vyžadována další zpoplatněná licence.



Obr. 4.19: GPON síť s modifikovaným (rougue) ONU

4.5.4 Výsledky měření

V rámci měření byly navrženy dva scénáře. První scénář se zabýval měřením na reálné síti[18] s obvyklým provozem, tedy v takové síti, kde ONU jednotky dodržují své přidělené sloty. Druhý scénář navazuje na první, avšak po čase byla připojena modifikovaná jednotka ONU (dále jen rogue ONU podle terminologie [53]). Nutno poznamenat, že rogue ONU se v druhém scénáři rozumí taková jednotka, která nerespektuje časové sloty.

Během měření prvního scénáře došlo k připojení nové, dříve nezaregistrované ONU, do sítě a odchycení veškeré komunikace mezi OLT a ONU, výsledky (jenž jsou zkráceny) jsou zobrazeny v tab. 4.6 a tab. 4.7. Připojená koncová jednotka musí projít celým aktivačním procesem (detaily jednotlivých stavů jsou v kapitole 4.4.2) a následně je umožněna datová komunikace. GPONxpert umožňuje analyzovat následující protokoly a procesy: signalizaci, OMCI (Optical netowrk unit Management and Control Interface – řídicí a kontrolní rozhraní v GPON sítích) kanál, Ethernet, IPv4 (Internet Protocol version 4 – internetový protokol verze 4), IPv6 (Internet Protocol version 6 – internetový protokol verze 6) a UDP (User Datagram Protocol – spojově neorientovaný protokol) komunikaci, podpora TCP (Transmission Control Protocol – spojově orientovaný protokol) chybí. Do této části byla vybrána pouze signalizace a UDP komunikace jako ukázka.

Druhý scénář s připojenou rogue ONU prakticky „eliminuje“ veškerou funkční komunikaci na síti, díky nerespektování časových slotů. Ostatní jednotky opakovaně

[18] Touto cestou bych rád poděkoval Ing. Lubošovi Dubravcovi ze společnosti Orange SK za to, že mi umožnil provést měření a jeho ochotu nadále spolupracovat.

Tab. 4.6: Detaily nově připojené ONU jednotky do sítě během registrační fáze

Čas	ONU-ID	Typ zprávy	Zdroj zprávy	Směr
00:00:11.806177	Nedostupné	SN ONU	PLOAM	↑
00:00:12.005427	Nedostupné	SN ONU	PLOAM	↑
00:00:12.198677	Nedostupné	SN ONU	PLOAM	↑
00:00:12.398927	Nedostupné	SN ONU	PLOAM	↑
00:00:56.698166	Nedostupné	SN ONU	PLOAM	↑
00:00:57.091666	Nedostupné	SN ONU	PLOAM	↑
00:00:57.290916	Nedostupné	SN ONU	PLOAM	↑
00:00:57.539500	Broadcast	Assign ONU-ID	PLOAM	↓
00:00:57.539625	Broadcast	Assign ONU-ID	PLOAM	↓
00:00:57.539750	Broadcast	Assign ONU-ID	PLOAM	↓
00:00:57.740125	2	Ranging Request	BWmap	↓
00:00:57.740161	2	SN ONU	PLOAM	↑
00:00:57.741500	2	Ranging Time	PLOAM	↓
00:00:57.741625	2	Ranging Time	PLOAM	↓
00:00:57.741750	2	Ranging Time	PLOAM	↓
00:00:57.777750	2	Configure Port-ID	PLOAM	↓
00:00:57.777875	2	Configure Port-ID	PLOAM	↓
00:00:57.778000	2	Configure Port-ID	PLOAM	↓

odesílají data, ale „nakažená“ ONU neumožňuje žádné odeslání dat, neboť odesílá data kontinuálně a OLT jednotka data očekává v časových slotech (nyní data přicházejí i mimo tyto sloty). Ze zachycených dat (viz tab. 4.8) je zřejmá absence veškerých identifikátorů a klíčových informací pro detekci takovéto jednotky. Z tohoto důvodu je nezbytné nalézt řešení pro odhalení takovéto ONU jednotky a její následné odpojení. Podle výsledků měření standardní sítě mohou být použity klíčové identifikátory (ONU-ID) k detekci libovolné ONU. Nicméně zásadní dokument [57] pro detekci rogue ONU obsahuje pouze dva scénáře, žádný z nich nedefinuje možnost změny firmwaru útočníkem, což je v dnešní době prakticky nejvýznamnější riziko. Standard připouští pouze dvě možnosti vzniku rogue ONU: MAC chybu a chybu vysílače s přijímačem. První uvedená možnost pokrývá špatně zavedený běh programu do FPGA pole (čímž nebude zajištěno očekávané chování ONU), anebo chybu vysílače s přijímačem, která je definovaná jako fyzické zapojení několika tranzistorů mezi Tx-pinem a zdrojem světla [57].

Tab. 4.8 zobrazuje data z analyzátoru GPONxpertu po jejich zpracování. Rogue ONU neodesílá ONU-ID, BWmap a GEM identifikátory. Bude-li bráno v potaz,

že rogue ONU využívá stále stejné hodnoty ONU-ID a Alloc-ID, pak mohou být tyto parametry použity pro detekci takovýchto jednotek. Nicméně výsledky jasně dokazují, že tyto identifikátory nejsou čitelné (modifikovaná ONU odesílá naprosto náhodná data).

Tab. 4.7: Datová komunikace mezi ONU a OLT v prvním scénáři

Čas	**Zdrojový port**	**Cílový port**	**Směr**
00:01:13.634783	DHCPv6 client (546)	DHCPv6 server (547)	↑
00:01:13.643500	DHCPv6 server (547)	DHCPv6 client (546)	↓
00:01:16.149662	39272	DNS (53)	↑
00:01:16.150158	39272	DNS (53)	↑
00:01:16.152500	DNS (53)	39272	↓
00:01:16.155875	DNS (53)	39272	↓

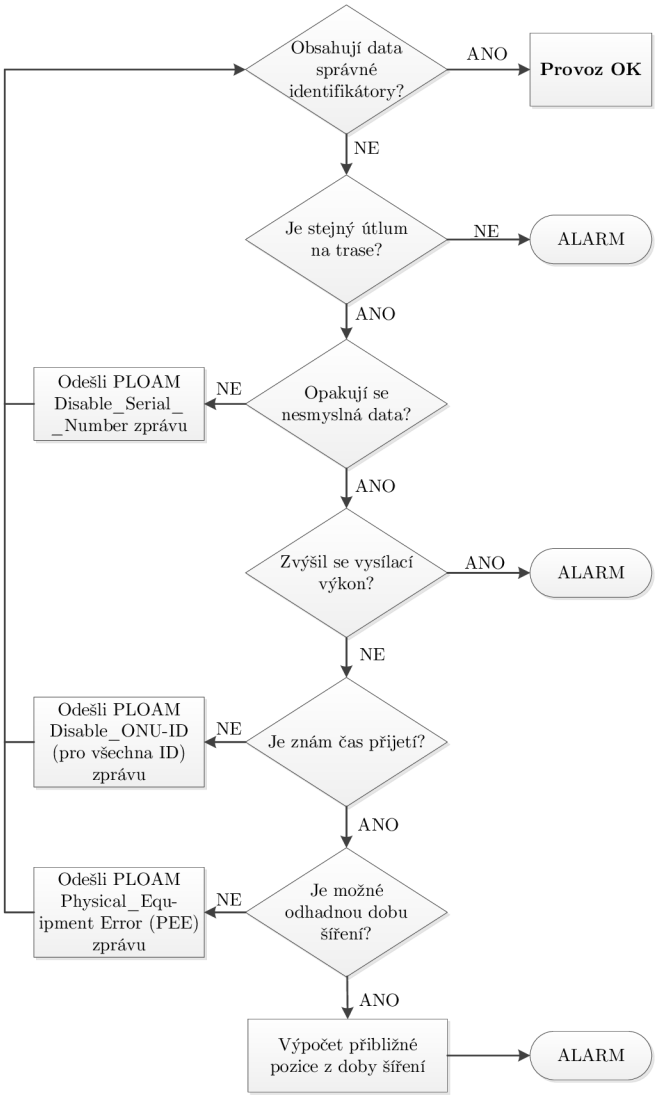
Tab. 4.8: Detaily provozu rogue ONU v reálné síti

Čas	**ONU-ID**	**PLOAM**	**BWmap**	**T-CONT**	**GEM**	**Směr**
00:01:08.14093	N.A.	N.A.	N.A.	253	N.A.	↑
00:01:08.14411	N.A.	N.A.	N.A.	253	N.A.	↑
00:01:08.14618	N.A.	N.A.	N.A.	253	N.A.	↑
00:01:08.14693	N.A.	N.A.	N.A.	253	N.A.	↑
00:01:08.15072	N.A.	N.A.	N.A.	253	N.A.	↑
00:01:08.15268	N.A.	N.A.	N.A.	253	N.A.	↑
00:01:08.15643	N.A.	N.A.	N.A.	253	N.A.	↑
00:01:08.15821	N.A.	N.A.	N.A.	253	N.A.	↑

4.5.5 Algoritmus pro detekci rogue ONU

V předchozí podkapitole byly prezentovány výsledky měření bez/s rogue ONU v síti. Prakticky nejhorším případem v reálné síti je připojení CW laseru s kontinuálním režimem na jeden ze vstupních portů na splitteru. Dostupný standard nepokrývá modifikovaný firmware na ONU jednotce, proto je nezbytné toto bezpečnostní riziko pokrýt například návrhem detekčního algoritmu, aby bylo zajištěno co nejrychlejší lokalizace a odpojení jednotky. Návrh takovéhoto algoritmu je zobrazen na obr. 4.20.

Navržený algoritmus startuje s ověřením unikátních identifikátorů, které má k dispozici každá ONU jednotka v distribuční síti (ONU-ID, Alloc-ID, T-CONT



Obr. 4.20: Nový algoritmus pro detekci rogue ONU

aj.). Pokud jsou identifikátory v pořádku (jsou čitelné), pak je provoz na síti v pořádku. Pokud nejsou, OLT zkontroluje útlum v distribuční síti za použití hodnot výkonových úrovní jednotlivých koncových jednotek (OLT uchovává historii těchto úrovní). V případě, že útlum není stejný (výkonové úrovně jsou jiné), pak OLT odešle zprávu do kontrolního centra (často označováno jako CO). V opačném případě se postoupí k další fázi (kontrole opakujících se nesmyslných dat). OLT obsahuje databázi se záznamy pro každou ONU (výkonová úroveň, ONU-ID, Alloc-ID, T-CONT aj.). Jakmile dojde k porovnání záznamů OLT v případě, že se nesmyslná data stále neopakují, odešle PLOAM zprávu Disable_Serial_Number. V opačném případě dojde k přechodu do další fáze (kontrole výkonové úrovně). V případě nárůstu výkonu, OLT informuje kontrolní centrum. Jinak OLT přechází

k další fázi v algoritmu, kde dochází k ověření, jestli je OLT schopno přečíst čas přijetí z GTC rámců. Z tab. 4.8 je zřejmé, že i přes absenci všech parametrů, je možné čas přijetí rámců přečíst. Pokud nelze stanovit čas přijetí, dojde k odeslání PLOAM zprávy Disable_ONU-ID. Další část algoritmu se zabývá stanovením propagačního zpoždění, pokud nelze toto zpoždění určit, OLT odešle PLOAM zprávu Physical_Equipment_Error. Poslední fáze vypočítá přibližnou polohu ONU za použití propagačního zpoždění. V potaz je brána hodnota typická pro jednovidová vlákna G.652 104 m/ µs. Poté OLT odešle report do kontrolního centra.

Odesílané PLOAM zprávy, první z nich Disable_Serial_Number, způsobí, že ONU přechází do tzv. Emergency Stop stavu. Jinými slovy ukončí přenos dat ve vzestupném směru. PLOAM zpráva Disable_ONU-ID zapříčiní vypnutí laseru a zahození ONU-ID, Port-ID a Alloc-ID. Přesněji řečeno ONU přejde do pohotovostního režimu. Poslední PLOAM zpráva Physical_Equipment_Error způsobí, že ONU aktivuje vlastní alarmy a vynuceně přechází do pohotovostního režimu. I samotná rogue ONU je schopna přijímat veškeré zprávy v sestupném směru, tedy i zpracovávat řídicí zprávy PLOAM.

Prezentovaný algoritmus a výsledky měření byly publikovány v [95].

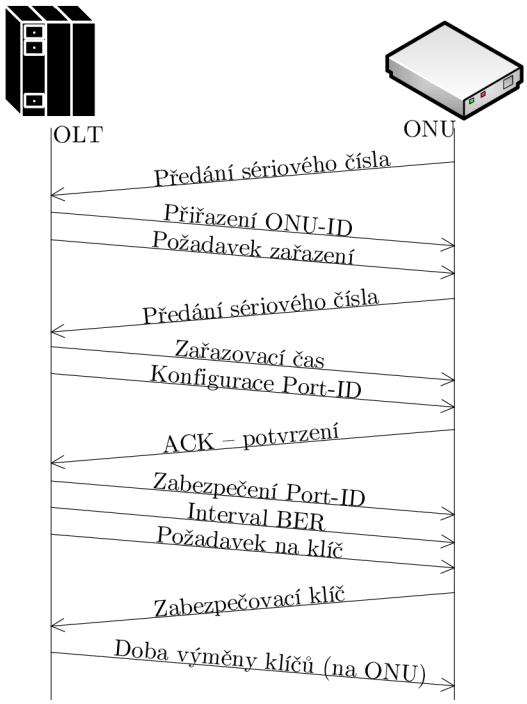
4.6 Analýza dat v GPON sítích

Analýza dat v reálné síti byla prováděna v síti operátora Orange SK[19].

Uživatelská data a kontrolní data jsou přenášena mezi OLT a ONU za pomocí rámců. Díky dalšímu zapouzdření není možné použít dostupné nástroje pro analýzu dat, jako je např. Wireshark. Bylo tedy nezbytné použít speciální měřicí přístroj GPONxpert ve standardním módu, který data ukládá na disk a teprve potom je umožněno další zpracování. Existuje i možnost data analyzovat v reálném čase, avšak pro tuto možnost je nezbytná další licence. Kontrolní data mohou být rozdělena do dvou částí: signalizační data a přenos OMCI. Nejdříve byla provedena analýza signalizačních dat z hloubkové analýzy obsahu rámce. Nutno poznamenat, že během fáze připojování jednotek jsou zprávy: přiřazení ONU-ID (Assign ONU--ID), konfigurace Port-ID (Configure Port-ID), přiřazení Alloc-ID (Assign Alloc-ID), zabezpečení Port-ID (Encrypted Port-ID), šifrovací klíč (Encryption_key), požadavek na klíč (key_request_message) a doba výměny klíčů (Key_switching_time) přenášeny celkem 3×. Posloupnost zpráv je patrná z obr. 4.21.

V analyzovaném vzorku jsou patrné PLOAM zprávy s názvem Serial number ONU, jenž byly přeneseny od ONU k OLT. Dále tato zpráva obsahuje

[19]Touto cestou bych rád znovu poděkoval Ing. Luboši Dubravcovi za ochotu a umožnění měření v síti tohoto operátora.



Obr. 4.21: Tok zpráv v měřené síti

ONU-ID = 255, což reprezentuje všesměrové vysílání (tedy všem ONU jednotkám) a dále obsahuje sériové číslo výrobce (v tomto případě 0x6A4F7431, identifikující společnost Huawei), seznam podporovaných profilů (GEM a/nebo ATM) a hodnotu náhodného zpoždění 79 µs. OLT jednotka měří čas mezi dvěma přijatými zprávami Serial number ONU a vyhodnotí odpovídající hodnotu zpoždění, které bude eliminovat následek rozdílné vzdálenosti jednotlivých koncových jednotek. Jakmile OLT přijme ONU-ID, odesílá zprávu Assign ONU-ID na základě unikátního zpoždění. Ačkoli OLT již zná přiřazené ONU-ID, stále není možné použít unikátní vysílání, neboť koncová ONU čeká na potvrzení svého ONU-ID. Při detailnějším prozkoumání obsahu rámce jsou patrné tzv. Psync (synchronizační část obdoba rámcového oddělovače); FEC indikátor s hodnotou 1 (data jsou opatřena dopředným zabezpečením chyb); ATM oddílem, který musí mít hodnotu 0 (ATM není podporováno na základě obsahu zprávy Serial number ONU) a BWmap částí rovnou 0, protože ONU jednotka nemá data k odeslání a zároveň nemá všechny nutné parametry pro realizaci komunikace.

Následně OLT odešle výběrovým vysíláním zprávu Ranging request s BWmap událostmi. Ranging požadavek je adresován unikátní ONU-ID (v tomto případě 2) s číselnou specifikací délky BWmap. Jinými slovy ONU je schopné použít jeden grant pro přenos dat. Dále ONU odpovídá zprávou Serial number ONU s použitím T-CONT třídy, indikující urgentnost dat. Po odeslání odpovědi, zprávou Ranging Time na požadavek Ranging, OLT vypočítá novou hodnotu ekvalizačního zpoždění. Dále OLT odešle zprávu Configure Port-ID specifické ONU jednotce. Tento identifikátor je velmi důležitý z pohledu přenosu dat, neboť je používán pro alokaci vybraných toků do jednoho GEM rámce. ONU musí odeslat potvrzení ACK ve stejném počtu, kolikrát přijalo zprávu (v tomto případě 3×). Jak může být viděno v tab. 4.9, zpráva DM_ID (Downstream Message Identification) obsahuje pole pojmenované „Configure Port-ID“ obsahující jméno potvrzované zprávy. Potom OLT zkontroluje, zdali Port-ID je zabezpečen nebo ne. V tomto případě Port-ID není zabezpečen, protože ONU je stále v registrační fázi. ONU potvrdí každou správně přijatou zprávu odesláním ACK. Později OLT odešle zprávu BER (Bit Error Rate – bitová chybovost), která definuje shluk intervalu pro ONU vyjadřující uvažovaný počet rámců v sestupném směru pro ONU pro výpočet množství chyb v sestupném směru. Nyní ONU zná pouze Port-ID, ale pro obousměrnou datovou komunikaci je dále vyžadován identifikátor Alloc-ID. Alokační identifikátor identifikuje množství datových entit, které mají svého příjemce a je nezbytné pro ně vyhradit část BWmap pole. Nutno poznamenat, že jediná ONU musí mít minimálně jeden Alloc-ID, který odpovídá hodnotě ONU-ID, tento identifikátor (s hodnotou odpovídající ONU-ID) není přenášen. V tomto případě OLT poskytlo 3 Alloc-ID identifikátory 258, 514 a 770 z alokačního rozsahu 256–4095. Jako obvykle ONU musí potvrdit přijetí každé PLOAM zprávy zprávou ACK. Následně je znovu zkontrolováno zabezpečení Port-ID, nicméně tato část je pouze volitelná, protože ve výchozím nastavením je zabezpečením dat vypnuto.

Obecně je datová komunikace po optických vláknech považována za bezpečnou, ale struktura GEM rámce a celkové zapouzdření dat je dobře známo [53]. Zabezpečená komunikace je inicializována OLT odesláním zprávy Request Key (pouze jednou). Zpočátku má ONU vlastní šifrovací klíč, když OLT odešle tuto zprávu, ONU potřebuje vygenerovat nový klíč. Nový klíč je vypočten na základě unikátního parametru, například sériového čísla ONU a poté je přenesen 3× k OLT ve zprávě Encryption Key. Je-li nezbytné klíč rozdělit do více zpráv, pak je použito fragmentace. OLT rozpozná po sobě jdoucí klíče díky fragmentačnímu indexu. První fragment (0–7 bajtů) z klíče má fragmentační index 0, pro další části je index inkrementován. OLT odpoví zprávou Key Switching Time se specifikací času (specifikuje StartTime a StopTime parametry v BWmap poli pro každé Alloc-ID). Následně dojde, po přečtení parametrů, k výměně klíče na straně ONU. V tomto případě

to znamená, že nový klíč bude použit od dalšího rámce s Alloc-ID 258 od 0–15 µs. ONU potvrdí každý rámec a od tohoto okamžiku je komunikace mezi OLT a ONU zabezpečena.

Tab. 4.9: Detaily zachycené GEM signalizace z analyzované sítě

ONU-ID	Typ zprávy	Zdroj zprávy	Směr	Podrobnosti
—	Serial number ONU	PLOAM Message	↑	ID výrobce = HWTC, SN výrobce = 0x6A4F7431, Náhodné zpoždění = 79 µs, Podpora ATM = vypnuta, Podpora GEM = povolena, ONU Tx výkonová úroveň = nízká úroveň.
Broadcast	Assign ONU-ID	PLOAM Message	↓	Psync = 0xB6AB31E0, Identifikace FEC identifikátoru = 1, BWmap = 0, ATM délka partice=0
2	Ranging Request	BWmap Event	↓	ONU-ID = 2
2	Serial number ONU	PLOAM Message	↑	Počet urgentních PLOAMu = 1, ONU-ID = 2
2	Ranging Time	PLOAM Message	↓	Psync = 0xB6AB31E0
2	Configure Port-ID	PLOAM Message	↓	
2	Acknowledge	PLOAM Message	↑	ONU-ID = 2, DM_ID = Configure Port-ID
2	Encrypted Port-ID/VPI	PLOAM Message	↓	Popisovač zabezpečení = Nezabezpečeno
2	BER interval	PLOAM Message	↓	ONU-ID = 2
2	Request Key	PLOAM Message	↓	ONU-ID = 2
2	Encryption Key	PLOAM Message	↑	Index klíče = 7, Index fragmentu = 0, Key Bytes = 0xCDE1D864096703CC
2	Key switching Time	PLOAM Message	↓	Alokační ID = 258, Pole začátku přenosu = 0 µs, Pole ukončení přenosu = 15 µs

4.6.1 Analýza OMCI kanálu

OAM (Operation, Administration and Maintenance – komunikace procesů, administrace a údržby) je přenášena uvnitř OMCI kanálu a je spuštěna co nejdříve po dokončení signalizační fáze. V případě analyzované sítě je k dispozici OAM kanál pro dvě ONU jednotky (v notaci výstupu jako ONU a ONU2). Bližší informace obsahuje tab. 4.10. OMCI procedury jsou inicializovány OLT jednotkou odesláním Get nebo Set požadavkem. Obecně, když OLT odešle Get nebo Set požadavek, ONU musí odpovědět s atributem Get/Set ve zprávě. Významná část OMCI analýzy je přenos obrazu softwarového nastavení, protože ONU je autorizováno vlastním sériovým číslem oproti OLT databázi (tato část je volbou operátora a jeho implementace). Nemá-li OLT jednotka záznam k odpovídajícímu sériovému číslu, pak ONU jednotce bude zabráněno stáhnout softwarový obraz s nastavením. Také je nezbytné uvést, že softwarových obrazů může být několik, a to podle klasifikace zákazníků, protože ne všichni zákazníci využívají stejné služby a jejich kombinace. Jakmile je ONU jednotka nahraje, pak je umožněno přenášet zákaznická metadata a podpůrná data služeb, například požadavek na veřejnou IP adresu nebo vyšší rychlost ve vzestupném směru atd. Dnešním trendem je kombinovat více služeb v rámci jednoho balíčku (jejich složení závisí na každém zákazníkovi). Každá služba je charakterizována rozdílnými požadavky na QoS, nejpřísnější požadavky na reálný provoz potřebují hlasové služby; proto ONU stáhne další konfigurační soubor pro hlasové

služby. Tento soubor obsahuje klíčové informace pro hlasové služby: použitý kodek, konstantní bitrate alokace šířky pásma a T-CONT prioritu.

Výše uvedené procedury OMCI kanálu patří mezi nejvýznamnější, ale OLT jednotka také používá tento kanál pro ověření synchronizace, indikaci alarmů (kupříkladu při ztrátě synchronizace) a monitorování FEC.

Tab. 4.10: Zachycené vzorky z OMCI kanálu z analyzované sítě

ID přenosu	Typ zprávy	Typ entity	Směr
10274	Get	(256) ONU G	↓
10274	Get Response	(256) ONU G	↑
10278	Get	(007) Software image	↓
10278	Get Response	(007) Software image	↑
10297	Get	(138) VOIP config data	↓
10297	Get Response	(138) VOIP config data	↑

4.6.2 Analýza Ethernet protokolu

Při detailnější analýze GPON payloadu lze detekovat Ethernetovou vrstvu a její komunikace. Na základě analýzy z přístroje TraceSpan GPONxpert bylo nalezeno několik zajímavých parametrů. Dostupné nástroje GPONxpertu, poskytují analýzu Ethernet prokolu, a to: číslo rámce, směr komunikace, čas přijetí rámce z média, VLANID (Virtual Local Area Network Identificator – identifikátor virtuální lokální sítě), zdrojovou a cílovou MAC adresu a identifikátor protokolu ze síťové vrstvy. Nicméně kompletní binární soubor není k dispozici.

V analyzované síti byla veškerá komunikace v obou směrech přenášena přes VLAN 836 a komunikace probíhala na druhé vrstvě[20]. Další anomálií je výskyt dvou shodných fyzických adres při komunikaci ve vzestupném směru. Na základě jedinečných identifikátorů OUI (Organizationally Unique Identifier – unikátní identifikátor organizace) odpovídají MAC adresy s prefixem E0:97:96 výrobci Huawei Technologies Co., Ltd, a proto lze očekávat, že se jedná o dvě fyzické OLT jednotky (případně jednu OLT s dvouslotovou kartou pro zákazníky) [96]. Cílové adresy jsou většinou pro IPv4 (01:00:5E) nebo IPv6 (33:33:00–33:33:FF) multicast [97]. Další cílová adresa v sestupném směru patří opět zařízení vyrobené společnosti Huawei Technologies Co., Ltd, tentokrát patřící ONU jednotce komunikující s jednou z OLT jednotek.

[20]GPON sítě disponují pouze fyzickou a spojovou/linkovou vrstvou, zastoupení dalších vrstev podle ISO/OSI modelu chybí.

Dále je patrný fenomén v sestupném směru, kde je několik Ethernet rámců detekovaných jako falešně pozitivní, z důvodu jejich hlavičky začínající kompletně náhodným obsahem. To vede k detekci chyb a nejedná se o Ethernet rámec na médiu. Protože nejsou k dispozici surová data Ethernet rámců, není možné provést detailní analýzu bit po bitu ani v jiném nástroji. V neposlední řadě také dochází k chybě i v CRC kódu těchto fantomních rámců, což je patrné z výstupu, viz tab. 4.11.

Tab. 4.11: Ukázka dekódovaných chyb na MAC vrstvě v sestupném směru

Cílová MAC adresa	**Zdrojová MAC adresa**	**Hexade. tvar**	**Směr**
CE:94:97:DC:C4:13	C5:70:9F:3D:1A:52	0x9C68	↓
BD:D8:4F:D5:F8:CE	8C:CC:EA:6C:26:CF	0x4713	↓
B0:2D:71:F9:A7:83	B3:52:D6:4D:E2:18	0x329C	↓
2B:0D:D5:C4:69:90	47:B0:5F:C2:A6:33	0x4561	↓
5C:58:34:AB:30:FF	9E:0F:7B:F1:C8:D5	0xF83E	↓
63:27:33:B5:80:54	95:D2:E8:6A:4C:06	0xADF4	↓
A9:AA:F3:FC:E1:7A	25:8D:02:BD:E3:D7	0xC314	↓
57:8A:41:57:31:B4	C5:0D:F0:C7:9A:DC	0x7D56	↓
05:71:06:B4:31:8D	69:EA:C5:BF:19:0C	0x9977	↓
73:A6:77:CD:FC:8B	C9:EC:6B:F8:E2:D9	0x88DA	↓
61:A2:09:4A:C4:D0	EA:EF:2F:70:68:79	0xB167	↓
C3:06:EE:42:83:F9	D4:A5:AE:6A:37:48	0xB06B	↓
94:AE:AB:BF:75:C4	19:30:11:9F:A0:C3	0x5F57	↓
25:90:A0:5E:7E:04	63:D7:16:EF:E2:68	0x5925	↓
1E:42:0B:69:F8:9C	68:1C:4C:2C:BE:24	0xA983	↓
B5:19:E3:32:AE:84	16:02:78:74:89:D6	0xE08	↓

4.6.3 Analýza síťové vrstvy provozu

Dále byla pozornost věnována analýze síťové vrstvy. GPONxpert rozlišuje mezi IPv4 a IPv6 provozem a poskytuje informace pro jednotlivé protokoly odděleně.

Pro IPv4 výstup obsahuje: čas příchodu paketu, celkovou délku v oktetech, zdrojovou a cílovou IP adresu, směr, další identifikátor protokolu a volitelné IPv4 hlavičky. Analyzovaná data zobrazují 31 dekódovaných IPv4 datagramů, dva z nich v sestupném směru odpovídající analýze z předchozí podkapitoly. Data byla odeslána na dvě IPv4 skupinové adresy, ale odpověď nebyla doručena. Zdrojová IP adresa (192.168.1.1) je privátní a nelze ji přenášet přes síť Internet, rozsah těchto nesměrovatelných adres je v [98] a cílová adresa je skupinová adresa (224.0.0.1) používaná pro

adresaci všem hostům na dané podsíti podle [99]. Užitečná data jsou identifikována jako IGMP (Internet Group Message Protocol – protokol pro skupinová vysílání) podle [100]. Datový provoz ve vzestupném směru je přenášen hostem, adresovaným s nesměrovatelnou veřejnou IP adresou (192.168.100.2) [98], která patří do jiné podsítě v sestupném směru, pokud bylo použito classful adresovací schéma [101]. Cílové IP adresy jsou v souladu s [99] zaměřené na všechny směrovače v dané podsíti (224.0.0.2) indikující jeden ze směrovacích protokolů, Link-local Multicast Name Resolution [102] (224.0.0.252) a Organization-Local Scope [103] (239.255.255.250). Opět následuje IGMP jako další protokol. Všechny pakety obsahují Router Alert IPv4 volbu [104], která označuje, že směrovače mohou vykonávat detailnější analýzu paketů. Router Alert IPv4 volba je použita v alokaci zdrojů napříč cestou IntServ, více detailů o této alokaci je v [105]. Zkrácený výstup z nástroje poskytuje tab. 4.12.

Tab. 4.12: Výstup z GPONxpertu pro IGMP protokol

Protokol	**Zdroj. IP adresa**	**Cíl. IP adresa**
Internet Group Management (0x02)	192.168.100.2	224.0.0.252
Internet Group Management (0x02)	192.168.100.2	224.0.0.2
Internet Group Management (0x02)	192.168.100.2	224.0.0.252
Internet Group Management (0x02)	192.168.100.2	224.0.0.252
Internet Group Management (0x02)	192.168.100.2	224.0.0.252
Internet Group Management (0x02)	192.168.100.2	224.0.0.2
Internet Group Management (0x02)	192.168.100.2	224.0.0.252
Internet Group Management (0x02)	192.168.100.2	224.0.0.2
Internet Group Management (0x02)	192.168.100.2	224.0.0.252
Internet Group Management (0x02)	192.168.100.2	224.0.0.252
Internet Group Management (0x02)	192.168.100.2	224.0.0.252

Obdobně jako pro IPv4 poskytuje nástroj analýzu dat i pro IPv6 až na podporu volitelných částí. Většina analyzovaných dat pro IPv6 pochází z datové komunikace, registrace skupinového vysílání, skupinové vysílání využívá lokální všesměrovou adresu (FF02::1) [106]. Analyzovaný vzorek dat poskytl informaci o zapouzdření IP protokolu [107] vše ve spojitosti za použití Multicast Listener Discovery protokolu v2 [108], označený cílovou adresou (FF02::16) [106].

4.6.4 Analýza transportní vrstvy

Z transportní vrstvy umožňuje nástroj dekódovat pouze UDP, ostatní protokoly transportní vrstvy jako TCP není možné řádně dekódovat, ačkoli se v daném provozu

nachází. UDP analýza poskytuje informace o: času příchodu datagramu, zdrojový a cílový port, délku payload a směr.

Analyzovaný vzorek obsahuje několik DNS (Domain Name System – systém doménovým jmen) přenosů, několik NATPMP (Network Adress Translation Port Mapping Protocol – protokol překladu adres) [109] a jedno DHCPv6 (Dynamic Host Configuration Protocol v6 – protokol pro automatickou konfiguraci zařízení v síti pod IPv6) [110] ustanovení. Výše uvedené výměny zpráv jsou procedurami síťového managementu a zobrazují málo informací o chování uživatelů. Pozorovaný vzorek dat odpovídá typické prvotní inicializaci uživatelské koncové jednotky.

Analýza přenášených dat v síti operátora Orange SK byla prezentována v [111].

4.7 Přenosová vrstva sítí nové generace

V současné době je největší pozornost stále věnována sítím podle standardu GPON. Nicméně ITU soustavně usilovně pracuje na novějších standardech, které zejména nabídnou vyšší přenosovou rychlost a dokáží překlenout vyšší dělicí poměr. Právě tento nový standard nese označení XG-PON[21], tedy pasivní optické sítě nové generace. Obecně je tento nový standard rozdělen na dvě studie: 10Gbit pasivní optické sítě a tzv. sítě NG-PON2, tedy sítě druhé generace.

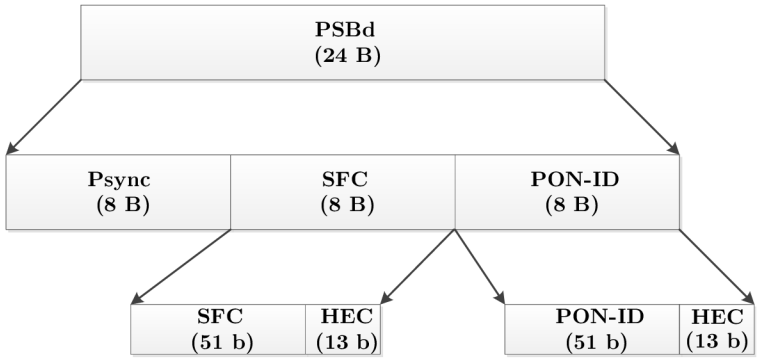
V rámci této sekce bude kladen důraz na sítě podle XG-PON, které nabízejí symetrickou a asymetrickou rychlost pro sestupný/vzestupný směr a je navýšen dělicí poměr z 1:64 (ačkoli GPON sítě teoreticky uvažovaly i 1:128) na 1:256. Navýšení dělicího poměru povede k modernizaci OLT a ONU jednotek a vyššímu důrazu na odolnost přenosové vrstvy. Rovněž pro datovou komunikaci při rychlostech vyšších než 10 Gbit/s je nezbytné uvažovat PMD (Polarization Mode Dispersion – polarizačně vidová disperze) [112].

Obdobně jako v kapitole 4.4 byl vytvořen simulační model v nástroji Matlab pro výpočet ekvalizačního zpoždění v závislosti na počtu ONU jednotek, neboť shodně s GPON sítěmi i XG-PON sítě disponují vyšším časem připojení jednotek v případě vyššího dělicího poměru. Čas připojení všech koncových jednotek závisí na jejich počtu a na čase připojování (chtějí-li být připojeny recipročně, doba klesá), v případě připojování více jednotek najednou doba roste. Problém kolize nastává v momentě připojení nové jednotky. Kolizní řešení není jasně specifikováno a neumožňuje kompletně zabránit kolizi v síti z důvodu nedostatečného rozsahu náhodného času pro připojení více ONU. Dále model simuluje vliv ekvalizačního zpoždění v závislosti na indexu lomu (standard udává obecnou hodnotu $n = 1,5$ bez rozdílů použité vlnové délky).

[21] Některé literatury udávají také název NG-PON nebo NG-PON1.

4.7.1 Aktivace ONU v sítích XG-PON

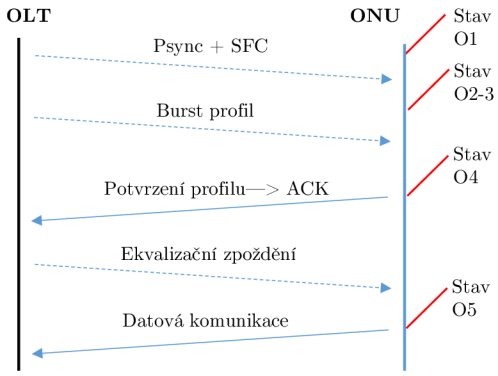
Princip aktivace koncových jednotek vychází ze stejných stavů jako síť GPON (popsáno v kapitole 4.4.2). Z tohoto důvodu bude následující popis zkrácen. Zpočátku jsou ONU a OLT jednotky neaktivní. Inicializační začátek synchronizace musí být zaveden v sestupném směru, když jsou ONU jednotky ve stavu O1. Synchronizaci zajišťuje synchronizační automat [113], aby došlo k synchronizaci, je nezbytná shoda 64bit z části PSync sekvence a hodnota z tzv. počítadla superrámců SFC (Super Frame Counter – počítadlo superrámců), jenž jsou definovány v hlavičce rámce v sestupném směru. Tato hlavička je označována jako PSBd a je zobrazena na obr. 4.22. Fyzický synchronizační block (PSBd) obsahuje 8B pole identifikující síť PON (za pomocí PON-ID) a obsahuje stejné pole jako SFC s 13bit hybridním zabezpečením dat HEC (Hybrid Error Correction – hybridní korekce chyb).



Obr. 4.22: Struktura synchronizačního pole PSBd v sítích XG-PON

Jestliže se v PON síti nachází více ONU jednotek, potom po přijetí Psync a SFC očekávají PLOAM, obsahující dostupné burst profily pro stav O2. Burst profil je reprezentován alokací dostupné šířky pásma ve vzestupném směru. Následně burst profily jsou alokovány pouze na požadavek. Informace o dostupných burst profilech jsou odesílány periodicky OLT jednotkou v intervalu stovek milisekund a více [113]. Na tyto nabídky profilů musí ONU reagovat potvrzením požadovaného profilu pro vzestupný směr. Jakmile OLT přijme a zpracuje potvrzení burst profilu odpovídající ONU, pak ONU přechází do stavu O4. Nyní ONU jednotka očekává alokaci ekvalizačního zpoždění (limitní doba přiřazení ekvalizačního zpoždění je dána časovačem TO1 = 10 s) a následně tuto alokaci potvrzuje. Po nastavení zpoždění se ONU jednotka přesune do stavu O5 (klíčové zprávy a parametry zobrazuje obr. 4.23).

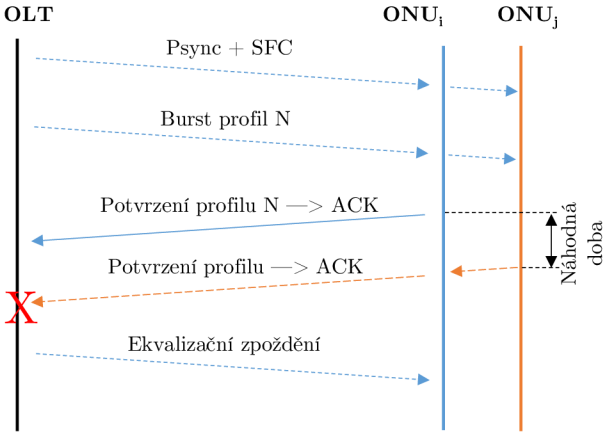
Celý výše uvedený text popisuje aktivační proces bez komplikací. Během komunikace může nastat výpadek, kupříkladu ztrátou synchronizace v sestupném směru LODS (Loss of Downstream – ztráta synchronizace v sestupném směru), následkem



Obr. 4.23: Klíčové zprávy pro aktivační proces jediné ONU

toho ONU přejde do stavu O6 a spustí časovač TO2 nastavený na hodnotu 100 ms [22]. Dojde-li k obnově synchronizace (synchronizační data OLT jednotka pravidelně odesílá), může se ONU jednotka vrátit do stavu O5. V opačném případě je nutný návrat do stavu O1 a zahájení celého aktivačního procesu od začátku.

Reálné sítě obsahují více než jednu koncovou jednotku ONU, které se připojují k OLT. Následkem toho probíhá více paralelních potvrzování dílčích burst profilů od všech těchto jednotek. K zabránění vzniku kolizí je náhodně vkládáno zpoždění v intervalu 0–48 µs. Nicméně pouze první potvrzený burst profil je přijatý, ostatní jsou zahozeny (viz obr. 4.24), přičemž čas odpovědí od každé ONU je limitován na 35±1 µs [23].



Obr. 4.24: Aktivační proces dvou ONU s kolizí

Nejhorším případem aktivace mnoho koncových jednotek najednou je výpadek elektrické energie. Synchronizaci v sestupném směru není možné obnovit do doby

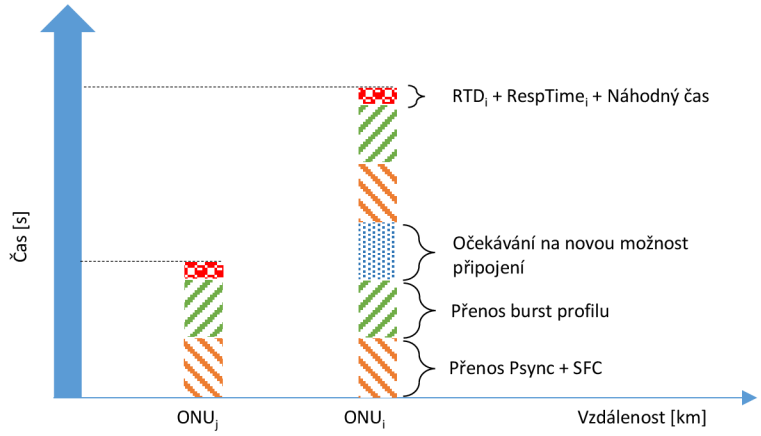
[22] Hodnotu mohou výrobci libovolně měnit.
[23] Hodnota je pevně daná a definována v [113].

TO2, neboť dojde k okamžitému výpadku OLT i ONU, přičemž OLT může mít zálohované napájení, nicméně ONU jednotky tuto možnost ve většině případů nemají. Budou-li, pro názornost, uvažovány dvě koncové jednotky, které chtějí být aktivovány ve stejný čas (po výpadku energie), budou postupně přijímat Psync, SFC a burst profil. Tyto informace jsou přenášeny periodicky výběrovým vysíláním. Celkově OLT obdrží dvě potvrzení profilu, ale pouze první jednotka bude aktivována. Jedná se ONU s nižším obousměrným zpožděním a menším vygenerovaným náhodným zpožděním. Oboucestné zpoždění je definováno jako přenos signálu k cíli a zpět ke zdroji. Lze jej pro XG-PON nadefinovat rovnicí (4.6) [113].

$$RTD_i = (n_{1310} + n_{1550}) \cdot \frac{L_i}{c}, \tag{4.6}$$

kde: c je rychlost světla ve vakuu, n_{1310} je index lomu na vlnové délce 1310 nm (1,451) a n_{1550} je index lomu na vlnové délce 1550 nm (1,448).

OLT zpracuje požadavek pouze první příchozí ONU jednotky a ta může přejít do stavu O4, ostatní setrvají ve stavu O2. Nepotvrzené jednotky opakují proces připojení. Na obr. 4.25 je zobrazen čas připojení jednotky ONU_j (připojena jako první) a časy nutné pro připojení koncové jednotky ONU_i.



Obr. 4.25: Časová závislost připojování více než jedné ONU jednotky

4.7.2 Nastavení simulací

Pro simulace XG-PON byla vytvořena jedna OLT jednotka, ke které se budou připojovat veškeré ONU. Pasivní optický splitter disponuje maximálním dělicím poměrem 1:256 v rámci útlumových bilancí a byly zachovány parametry definované standardem (např. doba pro odpověď maximálně 35±1 s). Spojení mezi splitrem a OLT jednotkou je realizováno standardním jednovidovým vláknem G.652 v délce

$L_{min} = 15\,km$. Vzdálenost mezi nejbližší a nejvzdálenější ONU je stanovena na $D_{max} = 5\,km$.

$$L_{\min} \leq L_i \leq L_{\min} + D_{\max} \tag{4.7}$$

V důsledku rovnice 4.7 je 256 ONU jednotek umístěno v okrajové vzdálenosti od OLT, přičemž jednotlivé vzdálenosti jsou generovány nástrojem Matlab náhodně.

4.7.3 Výsledky simulací

Kolizní systém v síti

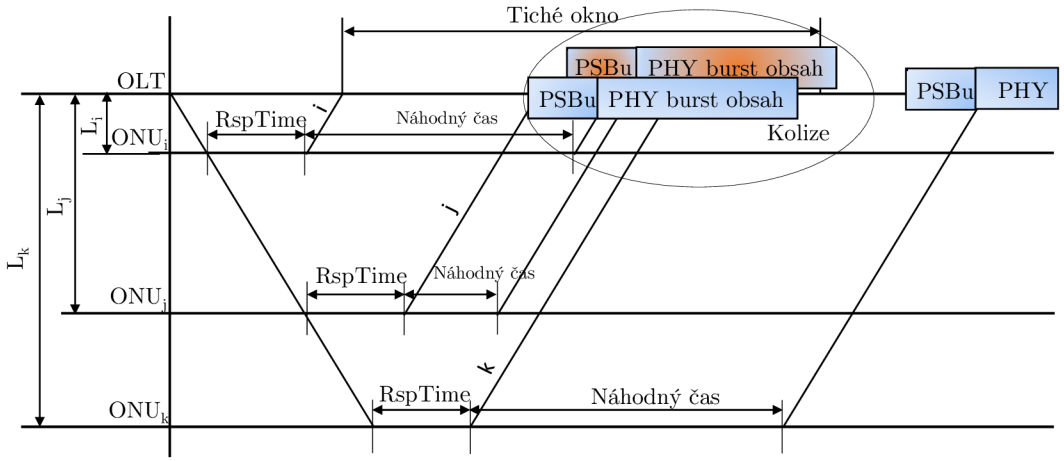
Jakmile je nová ONU jednotka připojena do sítě, může být zabráněno vzniku kolize přidáním náhodného zpoždění, které je zobrazeno na obr. 4.26 a také v [114]. Tento systém nevkládá náhodné zpoždění příliš efektivně, není možné tímto řešením zabránit většině kolizím.

Pokud je ONU_i ve vzdálenosti L_i a ONU_j ve vzdálenosti L_j od OLT, pak je možné zabránit kolizím přidáním náhodného zpoždění z intervalu 0–48 µs. Nicméně pravděpodobnost vzniku kolize narůstá s vyšším počtem koncových ONU jednotek na daném portu OLT jednotky, připojujících se ve stejném čase.

Druhá situace je reprezentována přenášením dat od OLT (z pohledu ONU v sestupném směru) pro nejvzdálenější ONU_{max} rámce N. ONU_{max} je umístěna ve vzdálenosti 19,9 km. Po 125 µs OLT odesílá rámec N+1 ONU_i, která je ve vzdálenosti 15 km. Rámec N (pro nejvzdálenější ONU) obsahuje informaci o ekvalizačním zpoždění s hodnotou StartTime = 77 µs, reprezentováno hodnotou 5989. ONU_{max} se nachází ve stavu O4 a odpovídá na příchozí rámec N s právě přiřazenou hodnotou StartTime. Následující rámec N+1 je odesílán výběrově (multicast metodou) a obsahuje nabídku profilu. Shlukový profil (burst profile) je použit pro zahrnutí nedávno připojených jednotek. Jednotka ONU_i, jenž přijala platnou hodnotu z Psync a SFC v předchozím rámci, může odpovědět. Odpověď je zpožděná o náhodnou dobu z intervalu 0–48 µs. Každá ONU jednotka vybere odpovídající hodnotu ze stejného rozsahu. OLT přijme rámce N a N+1 ve stejném čase, což je považováno za kolizní stav. Oba rámce jsou indikovány jako chyba a smazány. Výše uvedenou situaci lze vyřešit zavedením tzv. tichého okna.

Ekvalizační zpoždění

Jakmile je příslušný burst profil, přijatý ve stavu O2, potvrzen ONU, může dojít k přechodu do stavu O4, kde je očekávána alokace ekvalizačního zpoždění od OLT. V rámci simulací je ekvalizační zpoždění vypočteno z parametrů sítě. V této fázi je nezbytné znát hodnotu vzdálenosti od nejvzdálenější ONU jednotky od OLT.



Obr. 4.26: Detail vzniku kolize v síti XG-PON

Ekvalizační zpoždění pro libovolnou ONU je vypočteno na základě znalosti doby šíření signálu v sestupném a vzestupném směru mezi OLT a ONU, udávané rovnicí (4.8), kde T_{eqd} je konstanta doby odpovědi nejvzdálenější ONU_{max} a lze jej vyjádřit rovnicí (4.9) [113]:

$$EqD_i = T_{eqd} - (RTD_i + RspTime_i), \tag{4.8}$$

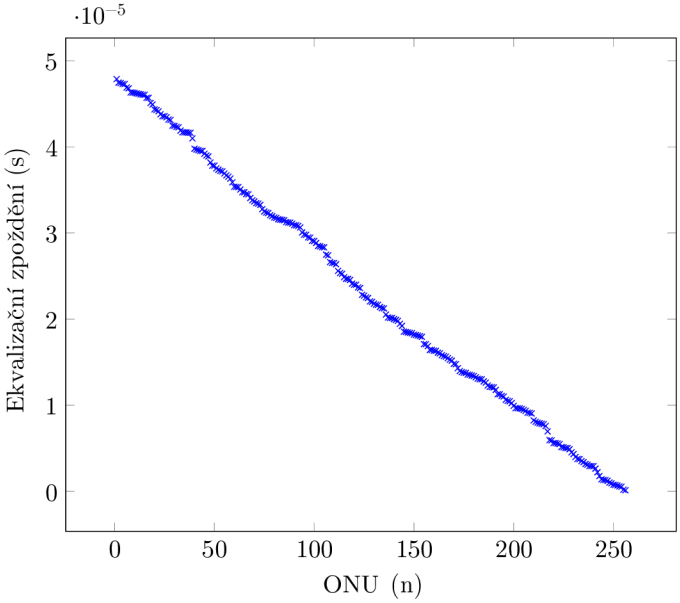
$$T_{eqd} = RspTime_{\max} + RTD_{\max}. \tag{4.9}$$

Rovněž je hodnota ekvalizačního zpoždění klesající, když přenosová vzdálenost roste. Výsledky simulací pro 256 ONU jsou zobrazeny na obr. 4.27. Nutno dodat, že jednotlivé vzdálenosti byly setříděny od nejmenší po největší.

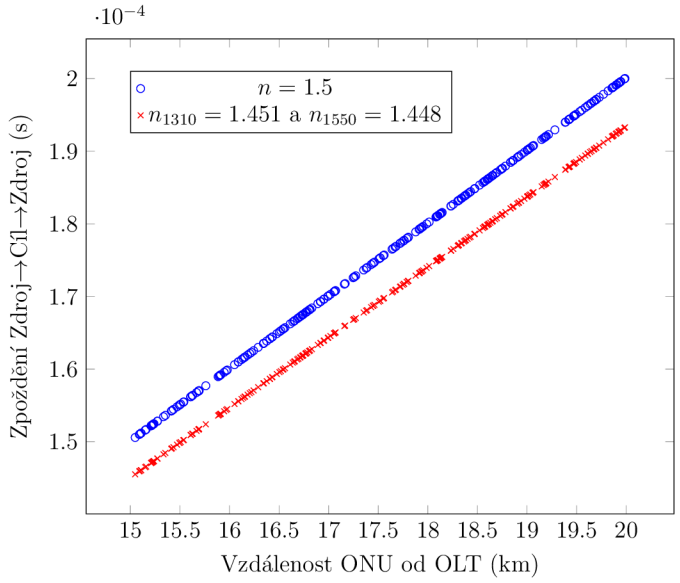
Vliv indexu lomu na dvoucestné zpoždění

V literatuře [113] a [114] je počítáno pouze s hodnotou indexu lomu $n = 1,5$. Tato hodnota je uvažována jak pro sestupný, tak pro vzestupný směr komunikace v XG-PON sítích. Bude-li brán v potaz standard jednovidových vláken G.652, pak je zřejmé, že je nezbytné znát obecný index lomu.

Oproti tomu výrobci jednovidových vláken udávají zcela rozdílné indexy lomu pro různé vlnové délky. Od výrobců vláken byly převzaty hodnoty indexy lomu a použity pro simulace závislosti dvoucestného zpoždění na vzdálenosti ONU jednotky. Simulace vycházejí z indexu lomu $n_{1550} = 1,448$ pro sestupný směr a $n_{1310} = 1,451$ pro vzestupný směr [115]. Výsledky simulací zachycující rozdílnost doby šíření jsou zobrazeny na obr. 4.28.



Obr. 4.27: Hodnoty ekvalizačního zpoždění v síti XG-PON s 256 ONU



Obr. 4.28: Vliv indexu lomu na obousměrné zpoždění v síti XG-PON

Je zřejmé, že celková doba poklesla, avšak pokles je udáván v jednotkách µs. Použití jednovidových vláken s nižším indexem lomu bude mít za následek až 5% zmenšení tzv. RespTime. Oproti tomu navýšení RespTime by mělo za následek nižší požadavky na HW jednotek. Druhou možností je zvýšení mezi-rámcové mezery pro redukování kolizí v síti.

Výsledky simulací byly prezentovány v [116].

4.8 ILP model PON sítě

V rámci studijní stáže na univerzitě Chongqing University of Posts and Telecommunications, ústavu telekomunikací pod vedením profesora Bao[24] byl vytvořen matematický model, jenž popisuje standardní chování Triple Play služeb v pasivní optické síti. Stromová topologie pasivních optických sítí umožňuje vytvoření pouze jednoduchého modelu, neboť ILP (Integer Linear Programming – celočíselné programování) je zaměřeno výhradně na orientované grafy. Základním nedostatkem ILP modelů je jejich komplexnost a časová náročnost na výpočet, nehledě na aktuální ceny výpočetních softwarů. Jakmile model dosahuje složitosti NP-kompletní, je zcela nezbytné k vyřešení použít heuristiku nebo problém rozdělit do dílčích částí a řešit je odděleně. Jako typický příklad NP-kompletní problematiky lze uvést problematiku RWA (Routing and Wavelength Assignment – problematika směrování a přiřazování vlnových délek) nebo řešení znovuobnovení spojení po zemětřesení v mesh sítích řešených např. v [117] a [118].

Nejběžnějším zapojením splitterů se rozumí kaskádové dělení, neboť dosáhnout využívání jediného splitteru s vysokým dělicím poměrem je značně neefektivní. Autoři se zabývají optimalizací rozmístění splitteru do kaskád za pomocí ILP modelu. Účelovou funkci tvoří celková cena výsledné topologie včetně všech komponent, omezenou o jediného rodiče pro každou ONU (v tomto případě OLT jednotku), vymezením celkového dělicího poměru v mezích standardů a využití pokud možno všech portů nadřazeného splitteru [119]. Na tuto publikaci navazuje [120] s rozšířením účelové funkce o využití erbiem dotovaných vláken, nicméně účelová funkce má stejnou úlohu, minimalizovat cenu řešení. Sítě druhé generace podporují vlnově přeladitelné lasery a výběrem vhodné vlnové délky se zabývá ILP model definovaný v [121]. Účelovou funkci tvoří minimalizace potřebného času pro přenos všech dat koncovým jednotkám. Model heuristiky tvoří dva algoritmy pro spravedlivé využívání vlnových délek napříč síti.

Hustě obydlené oblasti vyžadují dlouhodobé plánování rozvoje sítě. Při využití MILP (Mixed Integer Linear Programming – lineární programování včetně desetinných čísel) modelu prezentovaném v [122] lze úspěšné minimalizovat cenu výsledného řešení při maximální penetraci obyvatel. Nevýhodou tohoto modelu je vysoká náročnost pro řešení rozsáhlé sítě. Nejbližší uplatnění pro modelování PON sítě tvoří [123], kde je prezentován dynamické přidělování šířky pásma pro EPON sítě. Na druhou stranu řešení není přenositelné na sítě ITU standardů.

[24] I would like to express grateful thanks to my supervisor, prof. Ning-Hai Bao, Ph.D., for his encouragement, patient guidance, and advice during my two internships. You showed me the very interested topics and discussed with me everytime. Thank you so much!

4.8.1 Problematika přiřazení vlnových délek

Klasické datové sítě pracují s pakety, které jsou předávány mezi aktivními prvky. Výsledkem je přijetí paketu, kontrola cílové IP adresy a jeho následné odeslání přes zvolené rozhraní. Na druhou stranu optické sítě jsou data přenášená přes optické „crossconnect“[25], jenž každý přepíná optický signál, který je přenášen na různé vlnové délce do zvoleného směru. [124]

Pro aplikaci ILP modelu uvažujme následující scénář. Přiřazování vlnových délek je možné v rozdílných literaturách najít pod problematikou „barvení grafu“[26]. Při přiřazování vlnových délek jsou optické trasy vytvářeny na požadavek, kdežto jejich cesty jsou dané předem (tedy fyzickými optickými vlákny mezi prvky). Pokud dvě trasy sdílí jedno optické vlákno, pak je ustanovena hrana mezi odpovídajícími uzly. V jiném případě nedojde k ustanovení hran, neboť neexistuje sdílené vlákno mezi trasou. Jsou-li dva vrcholy připojeny k hranám, jedná se o sousedy. Vlnové délky odpovídají barvě v grafu. Přiřazení barev v grafu musí splňovat základní podmínku, že stejná barva není přiřazena dvěma sousedícím vrcholům. [124]

Principiální algoritmus může fungovat následovně [124]:

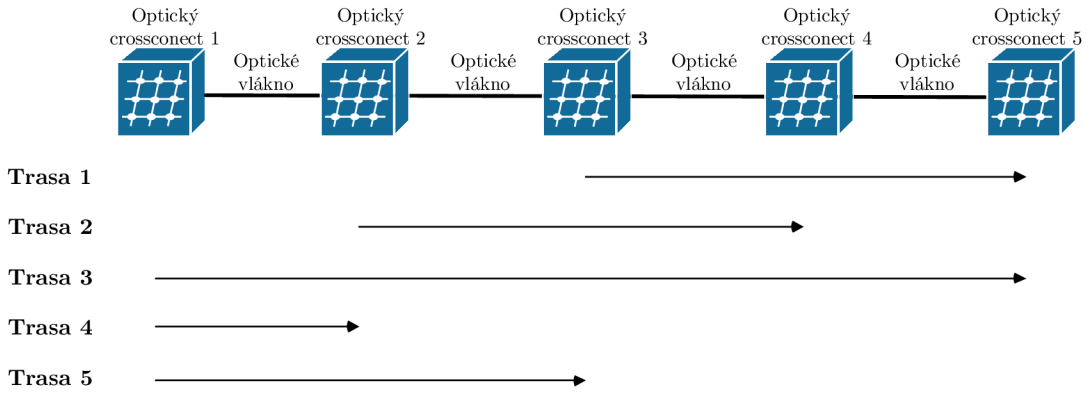
1. Inicializační fáze – dojde k inicializaci množiny vrcholů V a množiny hran E. Kde musí platit: $V \leftarrow \{\emptyset\}, E \leftarrow \{\emptyset\}$.
2. Generování vrcholů – musí dojít k vygenerování vrcholu v, který odpovídá každé optické trase a následně je přidána v do V. Tato část je zopakována pro každou optickou trasu.
3. Ustanovení hran – ustanovení hran (v, w) mezi $v \in V$ a $w \in V$, pokud dvě optické trasy odpovídají vrcholům v a w přenášených po stejném vlákně.

Výše uvedený scénář lze aplikovat na jednoduchý příklad zobrazený na obr. 4.29, který lze překreslit v rámci problematiky vybarvení grafu na obr. 4.30. Vrcholy v_i odpovídají optické trase i, jestliže optická trasa i a j sdílí stejné vlákno, pak jsou hrany (v_i, v_j) ustanoveny mezi v_i a v_j. Existuje-li (v_i, v_j) nelze přiřadit stejnou barvu oběma vrcholům. [124]

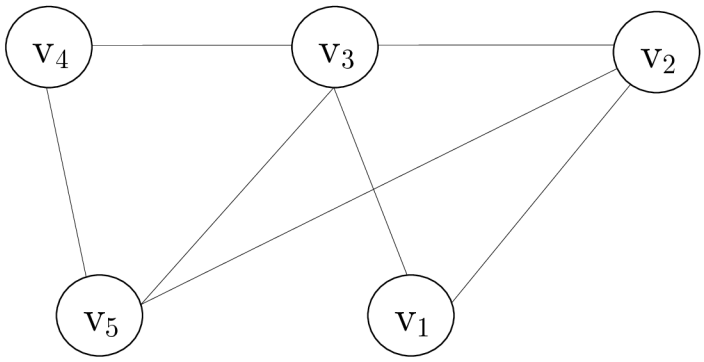
Model vybarvení grafu

Pro využití ILP modelu je nezbytné zpočátku nadefinovat použitou terminologii. Uvažujme W jako množinu možných vlnových délek λ, kde $W = \{\lambda_1, \lambda_2, \ldots, \lambda_{|W|}\}$. Dále je nezbytná definice binárních proměnných x_v^λ a y_λ. Jestliže λ je přiřazená cestě odpovídající v, $x_v^\lambda = 1$, v jiných případech $x_v^\lambda = 0$ a je-li λ použita minimálně jednou, pak $y_\lambda = 1$ jinak $y_\lambda = 0$.

[25] Ponechán anglický název z důvodu přesné terminologie.
[26] V anglické terminologii Graph coloring.



Obr. 4.29: Příklad požadovaných tras přes optické crossconects v síti [124]



Obr. 4.30: Požadované trasy v grafu [124]

Vybarvení grafu pak lze definovat jako ILP problém [124]:

$$\min \sum_{\lambda \in W} y_\lambda \tag{4.10}$$

S podmínkami [124]:

$$\sum_{\lambda \in W} x_v^\lambda = 1 \qquad \forall v \ \in V \tag{4.11}$$

$$x_v^\lambda + x_{v'}^\lambda \leq y_\lambda \qquad \forall (v, v') \in E, \forall \lambda \in W \tag{4.12}$$

$$y_{\lambda i} \geq y_{\lambda i\ +1} \qquad (i \ = 1, 2, \ldots, |W| - 1) \tag{4.13}$$

$$y_\lambda \in \{1, 0\} \qquad \forall \lambda \in W \tag{4.14}$$

$$x_v^\lambda \in \{1, 0\} \qquad \forall v \ \in V, \forall \lambda \in W \tag{4.15}$$

Rovnice (4.10) reprezentuje účelovou funkci, která má minimalizovat požadavky na vlnové délky/barvy. Podmínka (4.11) vyjadřuje, že každá optická trasa může použít jedinou vlnovou délku, omezení (4.12) předpokládá, že dva sousední vrcholy musí přijímat rozdílné vlnové délky. Prakticky se jedná o omezení využití stejné vlnové délky pro dvě trasy, jenž sdílí stejnou linku. Navíc omezení 4.12 udává, že x_v^λ nesmí překročit y_λ pro všechny $v \in V$, což znamená, že pokud $v \in V$ například $x_v^\lambda = 1$ existuje, pak y_λ musí být rovno 1. Podmínka (4.13) vyjadřuje, že vlnové délky jsou používány ve vzestupném pořadí $i \in W$. Poslední omezení (4.14), (4.15) vyjadřují možné hodnoty pro proměnné x_v^λ a y_λ. Po implementaci účelové funkce a všech omezení do softwaru např. glpsol, CPLEX nebo AMPL aj. je výsledkem rovnic hodnota 3, která reprezentuje minimální množství použitých vlnových délek. [124]

4.8.2 Triple Play model pro PON sítě

V rámci dosavadních standardů PON sítí je stále uvažována stejná vlnová délka na koncovou jednotku, přičemž [43] specifikuje využití i více vlnových délek za pomocí přeladění, kdy dojde k výměně stávající vlnové délky za jinou. Jinými slovy může dojít k výměně stávající OLT jednotky za jinou, má-li poskytovatel v provozu více souběžných OLT na jiných vlnových délkách. Každá koncová jednotka je uvažována jako zařízení, jenž realizuje převod optického signálu na elektrický a obráceně. Zdrojovými službami pro přenos do sítě Internet jsou stále 3 (data, hlas a video), tedy kombinace Triple Play.

4.8.3 ILP model Triple Play

V obecném hledisku se jedná o problematiku dostatečné šířky pásma pro přenos všech služeb. Jednotlivé služby jsou reprezentované požadavky jednotkami šířky pásma (obecně jsou služby definovány minimálními požadavky na přenosovou rychlost/kapacitu linku) a celková pasivní síť je limitována obecně kapacitou dané linky.

Model pro PON s Triple Play lze nadefinovat pomocí notace:

i	reprezentuje množinu všech ONU v přístupové síti.
j	reprezentuje množinu služeb (v tomto případě nabývá hodnot od 1 do 3) Triple Play služby.
C	udává maximální kapacitu linky před OLT.
W_j	reprezentuje požadované jednotky kapacity linky.
k_i	proměnná pro ONU jednotky se službou i.
$V_{i,j}$	proměnná typu služby s požadovanými jednotkami kapacity linky.

Úkolem účelové funkce, kterou prezentuje rovnice (4.16), je maximalizovat přenášený provoz s respektováním dostupné kapacity linky distribuční sítě. Kapacita linky je jediným limitujícím faktorem, neboť není k dispozici více vlnových délek. Celý ILP model pokrývá dosavadní možnosti GPON sítí. Účelová funkce je následně definována jako:

$$max \sum_{i \in I, j \in J} W_j \cdot V_{ij} + \sum_{i \in I} k_i \tag{4.16}$$

S podmínkami:

$$\sum_{i \in I, \ \ j \in J} W_j \cdot V_{ij} \leq C \tag{4.17}$$

$$V_{ij} = k_i \tag{4.18}$$

Pro účelovou funkci je nutné hlídat, aby nedošlo k překročení dostupné kapacity linky podle rovnice (4.17) a také přiřazování použitých služeb konkrétní ONU jednotce, jenž je nadefinovaná jako proměnná podle rovnice (4.18).

K vyřešení ILP modelu byl zvolen nástroj AMPL v rámci studentské licence, která je bohužel limitována počtem proměnných, iterací řešení a komplexnosti problému [125]. Řešitel, AMPL, je nástroj, který využívá pro nalezení řešení dva základní soubory: `.mod` a `.dat`. Soubor `.mod` obsahuje kompletní model v tomto případě reprezentovaný definováním množin a proměnných, účelovou funkci (viz rovnice (4.16)) a podmínkami (viz rovnice (4.17) a (4.18)). Samotný soubor `.mod` by nešlo přeložit, neboť neobsahuje žádné klíčové informace, tedy konkrétní hodnoty daných množin a proměnných. K těmto účelům slouží soubor `.dat`, jenž uchovává nadefinované hodnoty, jakožto vstupní parametry pro AMPL řešitele. V tomto případě soubor `.dat` obsahuje: množství jednotek ONU, počet služeb, kapacitu linky C a požadavky jednotlivých služeb podle W.

Pro spuštění řešitele AMPL je nutné zadat:

```
reset;
model ilp.mod;
data  ilp.dat;
solve;
display V,W,k,Bandwidth,Capacity;
```

Příkaz `reset;` zajistí, že nebudou ve výpočtu obsaženy žádné jiné uložené parametry nebo proměnné z jiných modelů. Pomocí `model ilp.mod;` dojde k načtení souboru obsahující model, tedy konkrétních definice proměnných a množin, účelové funkce a podmínek. Dále `data  ilp.dat;` přidají k modelu konkrétní hodnoty

všem proměnným a vymezí dané množiny. Klíčovým příkazem `solve;` dojde k výpočtu celého modelu bez zobrazení výsledku, výsledky je nezbytné zobrazit pomocí `display V,W,k,Bandwidth,Capacity;` (v závislosti na vlastní definici). Příkazem `solve;`, v případě úspěšného překladu a řešení, může být docíleno následujícího výpisu:

```
MINOS 5.51: optimal solution found,
19 iterations, objective 43.
```

Pro usnadnění celého postupu výpočtu byl vytvořen soubor `ilp.run`, který obsahoval výše uvedené příkazy pro spuštění. Tento soubor je spuštěn pomocí:

```
include ilp.run;
```

Řešení ILP modelu vede k optimálnímu řešení a je vhodné pouze pro malé sítě (v případě mesh sítí do 12 uzlů). V případě řešení větších/komplexnějších problémů je nezbytné využít heuristiku, která vyhledá suboptimální řešení. Nejčastěji je volena kombinace ILP a heuristiky.

4.8.4 Dosažené výsledky vlastního ILP modelu

Předešlá podkapitola se věnovala implementaci modelu do jazyku AMPL. Výpočet daného modelu probíhá po naplnění souboru `.dat` konkrétními hodnotami. Uvažujme nyní, že linka v ODN má kapacitu 64 jednotek, hlasová služba potřebuje 1 jednotku, datová služba 2 jednotky a video služba 3 jednotky pro přenos, celkový počet služeb vychází z Triple Play, tedy 3 služby na každou ONU, GPON sítě umožňují vydělit signál až pro 64 ONU, pro usnadnění výpočtu je uvažováno celkově 8 ONU jednotek.

Níže je uveden výpis ILP modelu z aplikace AMPL řešitele:

```
MINOS 5.51: optimal solution found.
24 iterations, objective 56
V~[*,*]
:   1   2   3    :=
1   1   1   1
2   1   1   1
3   1   1   1
4   1   1   1
5   1   1   1
6   1   1   1
7   1   1   1
8   1   1   1
;
:   W   k~:=
1   1   1
2   2   1
3   3   1
4   .   1
5   .   1
6   .   1
7   .   1
8   .   1
;
C = 0
```

Z výpisu je zřejmé, že hodnota C je rovna nule, neboť nedošlo k vyčerpání celé kapacity ani po přidělení všech služeb daným jednotkám. Jednoduchým součtem všech služeb na všech ONU docházíme k výsledku 48 jednotek, což nevyčerpalo dostupnou kapacitu linky C, a proto návratová hodnota je 0.

Ponechme parametry služeb shodné s definicí výše, ale po změně celkové kapacity linky C na nižší hodnotu než 48, například na 35, se výpis změní následovně:

```
19 iterations, objective 43
V~[*,*]
:   1   2   3    :=
1   1   1   1
2   1   1   1
3   1   1   1
4   1   1   0
5   1   1   1
6   1   1   1
7   1   0   0
8   1   0   0
;
:   W   k~:=
1   1   1
2   2   1
3   3   1
4   .   1
5   .   1
6   .   1
7   .   1
8   .   1
;
C = 1
```

Nyní je hodnota C rovna 1, protože došlo k celkovému vyčerpání kapacity linky a AMPL řešitel musel najít optimální řešení pro přidělení služeb všem koncovým jednotkám na síti. Navržený model není prakticky omezen počtem ONU jednotek, službami ani kapacitou, nýbrž výpočetními omezeními studentské licence programu AMPL.

Pokud by došlo k navýšení vstupních parametrů (proměnných) a jednotlivých podmínek, pak lze obdržet chybové hlášení ve znění:

```
Sorry, the student edition of AMPL is limited to 500 variables
and 500 constraints and objectives for linear problems.
You have 512 variables, 129 constraints, and 1 objective.
```

Z tohoto důvodu je možné AMPL řešitele použít pro řešení „malých“ problémů, co do počtu podmínek a vstupních proměnných. V ostatních případech je nezbytné zakoupit licenci.

Historicky významným uplatněním ILP modelu bylo v oblasti plánování železniční dopravy v Kanadě [126].

4.9 Implementace přenosové vrstvy NG-PON2

Neustálý nárůst požadavků na přenosovou rychlost a s tím související zvyšující se množství přenášených dat, které meziročně roste o 20–30 % [127], vede ke značnému navýšení přenosových rychlostí i v oblasti přístupových sítí. Posledním standardem pro PON sítě z dílny ITU je standard NG-PON2.

4.9.1 Dosavadní vývoj v oblasti NG-PON2

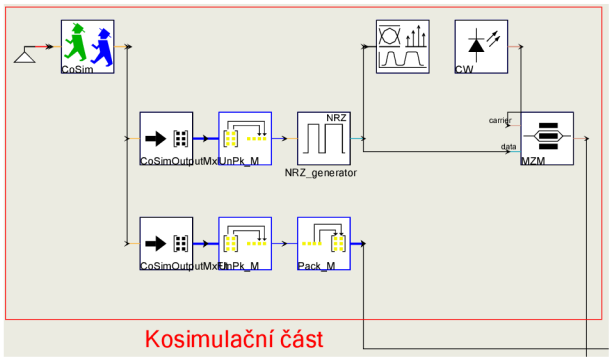
Stejně jako u předešlých standardů, ani u NG-PON2 není příliš velká pozornost věnována přenosové vrstvě, byť je na ní celá komunikace závislá. První článek se věnoval problematice úspory energie v NG-PON2 sítích [128], kde byly porovnány výsledky ILP modelu a algoritmu heuristiky. Hlavním nedostatkem je uvažování principu tzv. reportování a použití zpráv typu „gate“, jenž jsou využity v sítích na bázi Ethernet (NG-PON2 Ethernet rámce zapouzdřuje a tyto zprávy nevyužívá). Autoři [129] se zaměřili na optimalizaci aktivace koncových jednotek ONU, které nedosáhly přesného přeladění vlnových délek a přenáší data v jiném kanále. Jiná klíčová oblast ochrany infrastruktury pro přístupové sítě je uvedená v [130]. Článek poskytuje detailní přehled navržených redundantních topologií pro ochranu infrastruktury a zároveň definuje zasažené stavy v aktivačním procesu koncových ONU jednotek. Ačkoli redundantní schémata pro ochranu sítě byla již součástí GPON sítí, na poli výzkumu jim nebyla věnována velká pozornost. Myšlenka vlnově selektivní distribuční sítě se objevila v návaznosti na NG-PON2 v publikaci [131], kde je definováno využití vlnově-selektivních filtrů pouze pro vybrané oblasti, kde je vyšší počet koncových zákazníků, kdežto jiné oblasti stále dostačuje obsluhovat pasivními splittery. Další zkoumanou oblastí pro NG-PON2 jsou samotné transceivery, jelikož by měly být schopny dosahovat rychlého přeladění a musí podporovat přenosový režim v tzv. „shlucích“. Autoři [132] využili laditelný DBR (Distributed Bragg Reflector – laser s Braggovskými zrcadly) laser s dosahem 20 km, nízkou spotřebou energie a stabilní frekvencí v provozním režimu burst pro aplikaci v NG-PON2. Autoři [133] popisují možnosti využití NG-PON2 sítí jako metropolitních sítí v návaznosti cloudové služby. Jiné články se zaměřují na popis přenosové vrstvy v různých fázích standardizace finální podoby pro NG-PON2 [134], [135] a [136]. Celkový přehled vývoje pasivních optických sítí je popsán v [137].

4.9.2 Simulační model NG-PON2

Simulační model sestává z vysílací části OLT, distribuční sítě a přijímací části ONU. Základní implementace NG-PON2 využívá technologii TWDM-PON za použití 4 vlnových délek v každém směru, přičemž každá z nich je schopna přenášet

data rychlostí 10 Gbit/s. Počet přijímacích jednotek je závislý na zvoleném dělicím poměru.

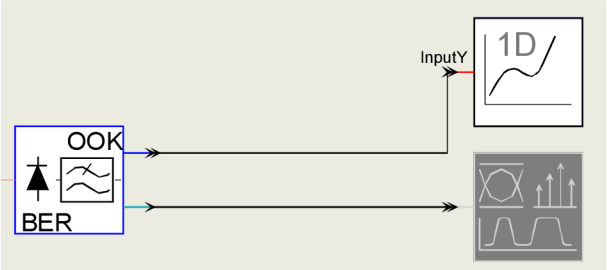
Vysílací část je realizována za pomocí 4 laserů (na obr. 4.31 pro ukázku je zobrazen jeden laser), které reprezentují jednotlivé vlnové délky a jsou dále kombinovány vlnovým multiplexorem. Generování dat a zapouzdření bitových sekvencí, odpovídající přenosové vrstvě NG-PON2, je implementováno v prostředí Matlab a dále přeneseno do prostředí VPIphotonics s využitím rozhraní „kosimulačního“ bloku. Tento signál se stává zdrojem pro modulátor. Vytvořené optické signály jsou dále multiplexovány a přenášeny do distribuční části sítě. Kosimulační blok disponuje dvěma výstupy, první výstup přenáší data do distribuční části sítě a druhý výstup je přiveden na vyhodnocení bitové chybovosti původní bitové posloupnosti.



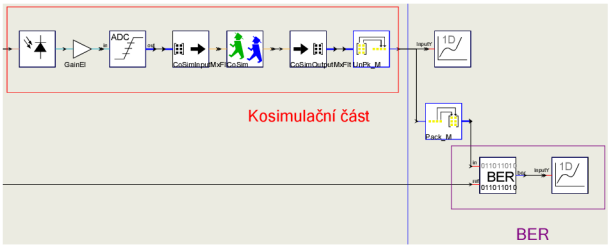
Obr. 4.31: Navržená vysílací část pro NG-PON2

Distribuční část je tvořena vláknem typu G.657, které je navrženo pro přístupové sítě (primárně pro vnitřní rozvody) s nízkým útlumem a vysokou odolností vůči ohybům.

Poslední část simulačního modelu tvoří přijímací část. Simulační model disponuje dvěma implementacemi měření bitové chybovosti. První implementace využívá stávající bloky z prostředí VPIphotonics (viz obr. 4.32). Druhá implementace se opírá o spolupráci VPIphotonics s prostředím Matlab a je zobrazena na obr. 4.33. Daná implementace konvertuje optický signál na elektrický, který je možné implementovat do prostředí Matlab pro další zpracování zapouzdřených dat a bitové chybovosti. Obě implementace mají za úkol stanovit bitovou chybovost, a tím určit provozuschopnost dané simulované sítě. Koncové prvky sítě NG-PON využívají jako fotodetektory lavinové diody (viz kapitola 1.3.2). V reálné síti jsou koncové jednotky přeladitelné, pro zjednodušení simulace tato část není implementována.



Obr. 4.32: Použité bloky z prostředí VPIphotonics pro výpočet BER



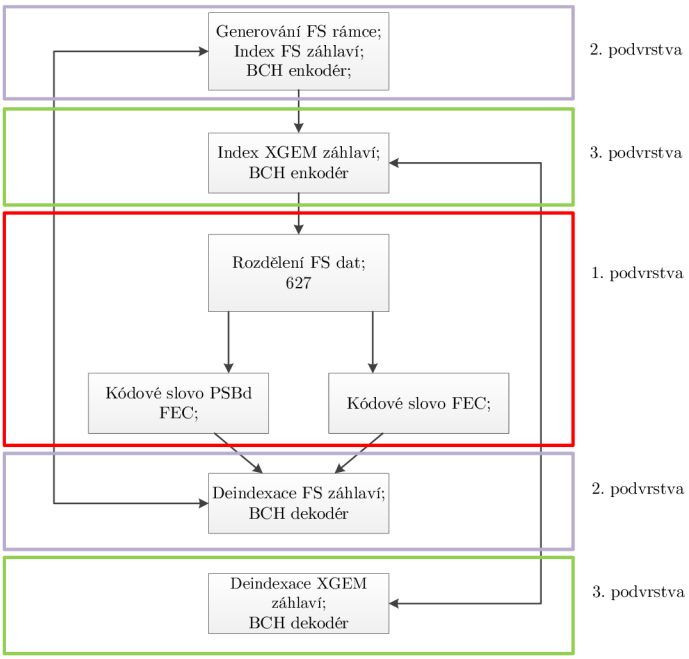
Obr. 4.33: Výpočet BER za použití kosimulačního režimu s prostředím Matlab

4.9.3 Detekce chyb pro NG-PON2 sítě

Jak již bylo zmíněno, přenosová vrstva PON sítí není implementována v žádném simulačním nástroji. Proto bylo nezbytné zajistit zapouzdření a odpouzření dat v externím programu Matlab a propojit obě aplikace v rámci kosimulačního bloku. Struktura implementovaného zapouzdření dat je zobrazena na obr. 4.34.

Jelikož velikost XGEM (XG-PON Encapsulation Method – zapouzdřovací metoda sítí nové generace) rámce v třetí podvrstvě je rozdílná a není shodná během zapouzdření, program začíná v druhé podvrstvě (známé jako rámcová podvrstva). Velikost rámce je 1 083 456 bitů a dále hlavička této podvrstvy obsahuje zabezpečení proti chybám HEC, což je kombinace BCH (Bose-Chaudhury-Hocquengham – cyklický zabezpečovací kód) a paritních bitů. Payload (užitečná data) je dále tvořen XGEM rámci a každý rámec je indexován a zabezpečen dodatečným 13bit HEC kódováním. Data na servisní adaptační podvrstvě obsahují identifikátory nezbytné pro správné doručení datového toku odpovídající koncové jednotce se správným rozlišením datových toků různých služeb (reprezentovaných jinými T-CONT). Přenášená data na druhé podvrstvě jsou rozdělena do 627 datových bloků a následně předána na první podvrstvu, kde jsou zabezpečena proti chybám a doplněna o synchronizační struktury[27]. Výsledkem je blok o velikosti 1728 bitů a po průchodu FEC

[27]Synchronizační struktury slouží k udržení synchronizace v sestupném směru pro všechny koncové jednotky. Vzorek dat je stále stejný.



Obr. 4.34: Model podvrstev v prostředí Matlab

kodérem se velikost zvětší na 1984 bitů. Na konci simulačního modelu je elektrický signál z fotodiody převeden do bitů a odpouzdřen za využití dekódování v prostředí Matlab. Výstupní bitová sekvence se porovnává s původní sekvencí na počátku. Teoretická přesnost bitové chybovosti je dána velikostí rámce na rámcové podvsrtvě, tedy $\frac{1}{1083456} = 9,229 \cdot 10^{-7}$.

4.9.4 Parametry simulované NG-PON2 sítě

Každá pasivní optická síť je charakteristická svou útlumovou bilancí. Aktuálně schválený standard NG-PON2 využívá 4 útlumové třídy, které zachycuje tab. 4.13 spolu s doporučenými výkonovými úrovněmi a citlivostí detektorů pro přenosovou rychlost 10 Gbit/s v sestupném směru.

Výkonové úrovně jsou uvedeny jako celkové, budou-li použity 4 vlnové délky, pak každá z nich bude mít 25 % hodnoty. V rámci simulačních scénářů byly vždy využity maximální hodnoty výkonových úrovní pro jednotlivé útlumové třídy. Konkrétní hodnoty pro simulace zobrazuje tab. 4.14.

Dalším klíčovým parametrem pro dosažení simulace reálné sítě jsou použité vlnové délky podle doporučení [45]. Pro účely simulace byly zvoleny vlnové délky podle tab. 4.15. Celkový útlum modelu je vypočten jako suma všech dílčích komponent a jejich útlumových hodnot.

Tab. 4.13: Útlumové třídy a jejich doporučené parametry

Útlumová třída	N1	N2	E1	E2
Minimální útlum [dB]	14	16	18	20
Maximální útlum [dB]	29	31	33	35
Min. výkon [dBm]	+3,0	+5,0	+7,0	+9,0
Max. výkon [dBm]	+7,0	+9,0	+11,0	+11,0
Minimální citlivost [dBm]	−28	−28	−28	−28
Maximální citlivost [dBm]	−7	−7	−7	−9

Tab. 4.14: Použité výkonové úrovně pro jednotlivé λ (celkem $4\,\lambda$)

Útlumová třída	N1	N2	E1	E2
Výkon jednotlivých λ [dBm]	1,75	2,25	2,75	2,75

Tab. 4.15: Použité vlnové délky pro simulaci přenosové vrstvy

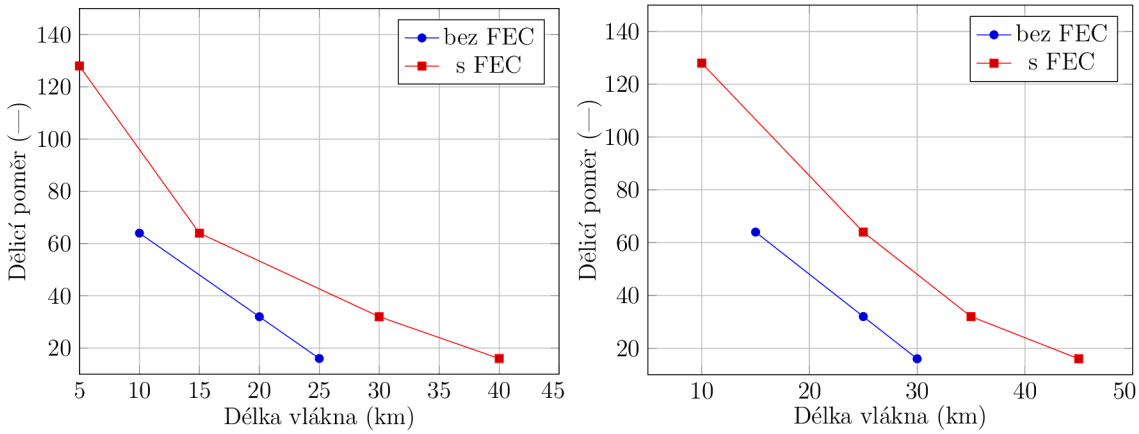
Kanál	Frekvence [THz]	Vlnová délka [nm]
1	187,8	1596,34
2	187,7	1597,19
3	187,6	1598,04
4	187,5	1598,89

Přesnost simulace je silně závislá na nastavení parametru *TimeWindow*, který reprezentuje množství dat přenášených přes jednotlivé komponenty simulace. V tomto případě byl tento parametr nastaven na hodnotu $2 \cdot 10^{20}$, při které byl průchod simulace stabilní. Pro zvýšení přesnosti výpočtu bitové chybovosti je možné využít vícenásobný průchod simulacemi, čímž dojde v každém průchodu ke zpřesnění výsledku BER. Vzhledem k tomu, že přenášené bity tvoří PHY (Physical interface – fyzické rozhraní/bitová posloupnost na tomto rozhraní) rámec s protichybovým zabezpečením, reálná bitová chybovost je dána jako velikost uživatelských dat v FS (Framing Sublayer – rámcová podvrstva/rámec této vrstvy) rámci na rámcové podvrstvě. Pro účely simulace byl FS rámec zredukován a limitní bitová chybovost je $2,192 \cdot 10^{-7}$, větší hodnoty BER simulační nástroj vyhodnotí jako 0. Na základě BER hodnot lze stanovit funkčnost/nefunkčnost simulovaného modelu.

4.9.5 Výsledky simulací

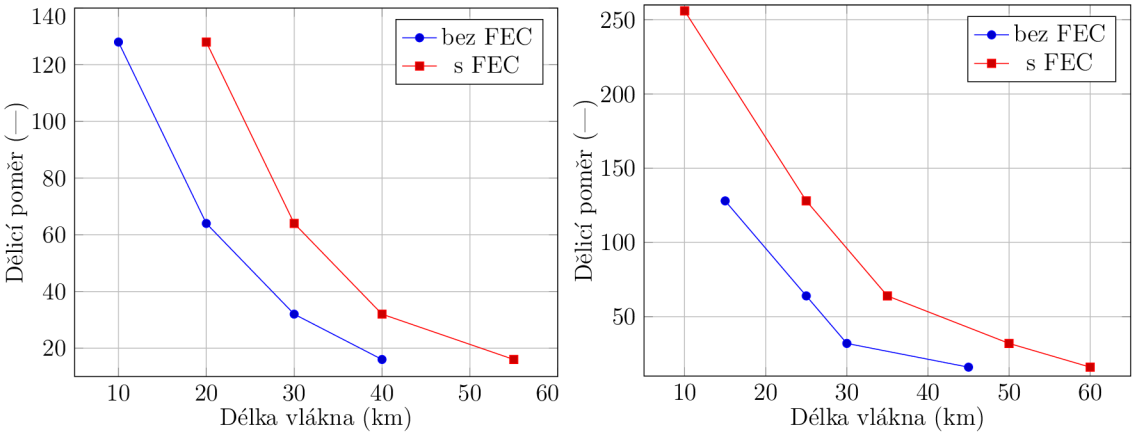
Veškeré simulace byly rozděleny zpočátku podle útlumových tříd definovaných v [45]. Podle teoretických předpokladů pro útlumové třídy ODN v tab. 4.13 lze vyvodit, že nejlepších výsledků dosáhne útlumová třída N1, neboť musí překonávat nejmenší útlum. Nicméně klíčovou roli hraje i maximální povolený vysílací výkon, který je naopak nejvyšší pro útlumovou třídu E2. Všechny simulace jsou provedeny pro základní dělicí poměry PON sítí 1:16, 1:32, 1:64 a 1:128. Přestože [45] uvádí i podporu dělicího poměru 1:256, nebyl tento poměr dělení brán v úvahu pro všechny simulace. V reálném nasazení je prakticky nulová pravděpodobnost, že by operátor využil jediného dělení 1:256, namísto obvyklého kaskádováního zapojení. Později v této podkapitole bude simulacemi dokázáno, že nejdelšího dosahu systému disponuje útlumová třída E2, kde byl nastaven maximální vysílací výkon na 11 dBm. Na rozdíl od útlumové třídy N1, která dovoluje maximální vysílací výkon pouze 7 dBm, čímž není kompenzován nižší útlum v porovnání s třídou E2. Na základě teoretických znalostí může být dosah systému prodloužen o 37 % s třídou E2 a nasazením vláken G.657 Allwave. Veškeré simulace byly vyhodnoceny na základě hodnot parametru BER. Je-li pasivní optická síť provozována bez protichybového zabezpečení, pak je limitní hodnota stanovena na 10^{-9}, kdežto s protichybovým zabezpečením může BER klesnout až k hodnotě 10^{-4} před korekčním kódováním.

Komerčně dostupné simulační nástroje se stále zaměřují především na fyzickou vrstvu. Z tohoto důvodu byla implementována přenosová vrstva sítí druhé generace, aby bylo možné simulovat oba reálné případy (byť je protichybové zabezpečení volitelnou položkou). Výsledky simulací podle obr. 4.35 dokazují teoretické předpoklady, že protichybové zabezpečení dokáže významně prodloužit dosah celého systému. Pro dělicí poměr 1:64 dosahuje celý systém maximálně 10 km, kdežto při použití protichybového zabezpečení se dělicí poměr navyšuje až na 1:96.



Obr. 4.35: Průběh spolehlivého přenosu v rámci útlumových tříd N1 a N2

Není přitom relevantní, jestli bude využito jednoho vydělení nebo kaskádního zapojení. Minimální dělicí poměr pro prodloužení dosahu byl uvažován poměr vydělení 1:16, kde výsledky dokazují dosah 25 km respektive 40 km (s protichybovým zabezpečením). Výsledky útlumové třídy N2 vykazují ještě vyšší dosah systému, nicméně to je způsobeno vyššími vysílacími výkony. Dělicí poměr 1:64 bez zabezpečení lze provozovat až na 15 km v porovnání se stejnou vzdáleností se zabezpečením je možné dělicí poměr navýšit na téměř dvojnásobek.



Obr. 4.36: Průběh spolehlivého přenosu v rámci útlumových tříd E1 a E2

Výběr vhodné útlumové třídy probíhá během plánování penetrace a je závislá na dodané technologii. Jednotlivé standardy vždy definují 4 základní útlumové třídy a mnohdy dodají i další – rozšiřující. Výsledky druhé poloviny útlumových tříd (E1 a E2) jsou zobrazeny na obr. 4.36. Jak již bylo zmíněno, nominální útlumové třídy (označené N) musí překlenout menší útlum než rozšiřující třídy (v zápise uváděny počátečním písmenem E). Při porovnání výsledků třídy E1 je patrné, že zabezpečení proti chybám umožní využívat druhý největší dělicí poměr (1:128) do vzdálenosti 20 km versus 10 km bez korekce chyb. V porovnání s E2, kde je možné využít dělicí poměr 1:256 do vzdálenosti 10 km s korekcí chyb, bez této korekce není možné vůbec tento poměr dělení nasadit. Nejmenší simulovaný poměr (1:16) je možné bez zabezpečení implementovat do vzdálenosti 40 km (E1) respektive 45 km. Při zabezpečení dat se dosah ještě prodlouží na 55 km (E1) respektive 60 km (E2).

Implementovaný vrstvový model z prostředí Matlab prodlužuje celkový dosah systému na principu NG-PON2.

Prezentované výsledky jsou v době odevzdání dizertační práce v recenzním řízení v [138].

5 ZÁVĚR

Cílem dizertační práce bylo představit základní parametry pasivních optických sítí. Počáteční pozornost je věnována historickému měření rychlostí světla. Aktuální hodnota rychlosti světla $c = 299\,792\,458\,\mathrm{m/s}$ vycházela z několika pokusů a omylů. Průkopníkem byl italský fyzik Galileo Galilei, jenž uskutečnil první měření za pomocí dvou lucern, nicméně tento pokus skončil neúspěchem. Úspěšným navázáním na Galileiův pokus uskutečnil dánský astronom Ole Roemer. Výsledkem pokusu byla hodnota $c = 2,2 \cdot 10^8\,\mathrm{m/s}$, a to již v roce 1676. Veškeré, do té doby, realizované pokusy byly realizovány mimo laboratorní prostředí. Výsledkem laboratorního měření byla hodnota $c = 3,13 \cdot 10^8\,\mathrm{m/s}$. Další upřesnění hodnoty, s navázáním na předešlé výsledky, uskutečnil francouzský vědec Jan Focault v roce 1862, s výsledkem $c = 2,977 \cdot 10^8\,\mathrm{m/s}$. O větší zpřesnění hodnoty, a prakticky nynější hodnotu, se postaral americký vědec Albert Abraham Michelson. V rámci této kapitoly jsou popsány klíčové fotodetektory pro pasivní optické sítě a jejich fyzikální princip.

Pasivní optické sítě jsou stále aktuálním tématem vzhledem k tomu, že jsou nejčastěji nasazovány jako klíčové technologie pro dosažení maximální přenosové rychlosti v oblasti přístupových sítí. Přestože se dnes objevuje celá řada standardů, stále je velmi oblíbeným, prakticky 12 let starý, gigabitový standard nazývaný GPON. Praktickým a reálným důvodem nasazení tohoto standardu jsou doposud nejdostupnější finanční náklady. Přestože je několik kapitol věnovaných gigabitovému standardu, poslední tři kapitoly se věnují i novějším standardům.

Česká republika, jakožto člen Evropské unie, se zavázala k rozšíření širokopásmového připojení k Internetu, a to s minimálními rychlostmi 30 Mbit/s pro současné klienty a 100 Mbit/s pro nové zákazníky. Podle výsledků průzkumu ČTÚ (Český telekomunikační úřad) z roku 2016, je stále dominující technologie připojení k Internetu pomocí bezdrátového spoje, nejčastěji WiFi. Přípojky pomocí optického vlákna (libovolně zakončeného) zaujímají pouze 11,9 % všech přípojek. Dosavadní publikace ČTÚ se ubíraly i směrem vhodné technologie pro naplnění cílů EU. Libovolné zakončení optického vlákna nabízí dostatečnou šířku pásma a přenosovou rychlost i pro budoucí aplikace, které se budou ubírat zpravidla streamováním videa, online přenosy (nejen prezentací/přednášek, ale v současné době i her). Výhledově lze GPON standard označit jako dostačující v horizontu 2–5 let, přičemž lze navýšit přenosovou rychlost snížením dělicího poměru na jednom portu OLT. Nutno však podotknout, že druhým limitujícím faktorem je rychlost uplink (dosavadní chassis podporují rychlost do 40 Gbit/s).

Nejdiskutovanějším tématem v oblasti GPON je stále bezpečnost. Bezpečnosti v ohledu datové komunikace je docílené implementací algoritmů, nicméně výchozí stav veškerých OLT jednotek je komunikace v nešifrované podobě. Přenášené rámce

mají značně složitou metodu zapouzdření z Ethernet rámců do GEM rámce, typické pro komunikaci napříč distribuční sítí. Jako druhý příklad lze uvést autentizaci ONU vůči OLT, která je nezbytná, obrácená autentizace není zvažována, proto tzv. „podvržené“ OLT může komunikovat se všemi koncovými jednotkami. Správa hesel v OLT jednotce je značně komplikovaná a uložená hesla zobrazují v konfiguračním souboru pouze hash všech hesel. Bohužel jakékoli heslo je šířeno v rámci PLOAM zprávy, ve výchozím režimu, v holé textové podobě. Jeden z cílů dizertační práce si klade za cíl zvýšení bezpečnosti za pomocí parametru T_{prop}. Centrální jednotka OLT využívá známých časů odeslání/přijetí GEM rámce pro výpočet tzv. ekvalizačního zpoždění, jenž eliminuje rozdílné vzdálenosti koncových jednotek. Při ustanovení hesla koncová jednotka musí poskytnout jisté unikátní parametry, navržený model umožňuje využít parametr T_{prop} jako unikátní složku klíče. Měřením byla ověřena funkčnost modelu a výsledky prokazují, že doba 270 µs odpovídala době zpracování signálu v kartách se SFP+ (Small Form-factor Pluggable Plus – zásuvný SFP modul s rychlostí 10 Gbit/s). Dílčím výsledkem je stanovení doby 8 µs pro každý 1 km optického vlákna. Dosahovaná přesnost odpovídá cca 120 m, což znamená, že sousedi na stejném patře mohou mít velmi podobnou hodnotu parametru. Tento nedostatek lze odstranit zvýšením přesnosti měření parametru v jednotkách „ns“. Na tento model navazuje tzv. „robustní“ model zabezpečení, jenž je rychlejší než současné modely.

Čtvrtá, pátá a šestá podkapitola z praktických výsledků se zabývají aktivačním procesem koncových jednotek, principem komunikace v GPON sítích a analýzou přenášených dat. Současný aktivační proces koncových jednotek po výpadku elektrické energie značně prodlužuje opětovnou komunikaci řídicí jednotky a koncové jednotky. Aktivační proces je reprezentován 7 stavy, přičemž pro komunikaci je klíčových pouze 5. Počáteční stav je inicializační, koncová jednotka pouze naslouchá, poslední, pátý stav, je konečným stavem, kde koncová jednotka může přenášet data v obou směrech. Na jedné kartě OLT jednotky s 8 SFP sloty, může být obsluhováno až 1024 koncových jednotek. Cílem simulací bylo vytvořit model v Matlabu pro výpočet aktivace poslední jednotky na daném slotu. Současný algoritmus aktivuje 128. jednotku po cca 133 s. Při plném obsazení OLT karty se doba prodlouží na ≈17 min. Nově navržený algoritmus umožní tento čas zkrátit na 6,5 s pro 128 koncových jednotek a 52 s při plném obsazení OLT karty. Další podkapitola si kladla za cíl zmírnit významné bezpečnostní riziko, detekovat modifikovanou koncovou jednotku ONU, která nerespektuje přidělené časové sloty. Modifikovaná jednotka byla připojena do sítě Orange SK a provedeny náměry pomocí nástroje GPONxpert. Z náměrů byl navržen postup pro detekci této koncové jednotky. Navazující podkapitola vychází z podobného principu měření, avšak bez modifikované jednotky. Podkapitola shrnuje teoretický popis komunikace jak v sestupném, tak vzestupném směru. Analýzou přenášených dat bylo docíleno identifikace klíčových

požadavků (stažení konfiguračního souboru aj.).

Sedmá podkapitola se věnuje přenosové vrstvě sítí další generace z pohledu aktivačního procesu. Význam ekvalizačního zpoždění je eliminace různých vzdáleností ONU jednotek z pohledu OLT. Druhým cílem bylo posouzení vlivu indexu lomu na obousměrné zpoždění v sítích XG-PON. Aktuální standardy a publikace neustále využívají pouze obecný index lomu, přičemž tento parametr je silně závislý na použité vlnové délce. Simulacemi bylo docíleno porovnání obou hodnot.

Navazující podkapitola přináší matematický model xPON sítí přenášející Triple Play služby (data, video a hlas). K tomuto účelu byl vytvořen ILP model, který obsahuje definici: ONU jednotek, množinu přenášených služeb, maximální kapacitu linky pro danou ODN a požadavky kapacity pro přenos dané služby. Účelovou funkci tvoří maximalizace přenášených služeb. Veškeré ILP modely mají za cíl nalezení optimálního řešení pro danou účelovou funkci. Nadefinováním počtu ONU jednotek, kapacity linky a požadavků služeb bylo pomocí *ampl* řešitele docíleno optimálního rozdělení služeb s maximálním možným využitím kapacity linky.

Poslední podkapitola je zaměřena na implementaci přenosové vrstvy do komerčně dostupného simulačního nástroje VPIphotonics. Tento nástroj je určen převážně pro simulace fyzické vrstvy bez jakékoli podpory vyšších vrstev. Implementované zabezpečení, založené na dopředném kódování FEC, bylo vytvořeno v externí aplikaci Matlab a dále spojeno s nástrojem VPIphotonics pomocí kosimulačního bloku. Simulacemi bylo docíleno výrazné prodloužení distribuční sítě, a to zcela bez využití jakéhokoli optického zesilovače. Výsledky pro útlumovou třídu N1 prokázaly navýšení dosahu ODN o 15 km, z 25 km na 40 km. Tato útlumová třída musí překonat nejmenší útlum v ODN, nicméně je povolen také nejnižší vysílací výkon. Naproti tomu v síti s útlumovou třídou E2, lze dosáhnout cca 46 km bez zabezpečení nebo 60 km se zabezpečením. Hlavním kritériem vyhodnocení byla bitová chybovost. Limitní hodnota bez zabezpečení odpovídá 10^{-9}, se zabezpečením pak lze tolerovat BER do hodnoty 10^{-4}.

LITERATURA

[1] GALILEI, Galileo a Maurice A. FINOCCHIARO. *The essential Galileo*. Indianapolis, Ind.: Hackett Pub. Co., c2008. ISBN 978-0-87220-937-4.

[2] GALILEI, Galileo a Stillman. DRAKE. *Discoveries and opinions of Galileo: including The starry messenger (1610), Letter to the Grand Duchess Christina (1615), and excerpts from Letters on sunspots (1613), The assayer (1623)*. 24th Edition. New York: Anchor Books, 1990. ISBN 978-0385092395.

[3] COHEN, I. Bernard. *Roemer and the first determination of the velocity of light*. Burndy Library, 1944. ASIN B0007FM1GO.

[4] BURNIE, David. *Light*. New York: Dorling Kindersley, 2000. ISBN 978-0-7894-6709-6.

[5] AL-AZZAWI, Abdul. *Photonics: principles and practices*. Boca Raton, FL: CRC Press, c2007. Optical science and engineering (Boca Raton, Fla.), 123. ISBN 978-0-8493-8290-1.

[6] BRECHER, Kenneth. Is the Speed of Light Independent of the Velocity of the Source? *Physical Review Letters*. 1977, **39**(17), 1051–1054. DOI: 10.1103/PhysRevLett.39.1051. ISBN 10.1103/PhysRevLett.39.1051. Dostupné z URL: <`http://link.aps.org/doi/10.1103/PhysRevLett.39.1051`

[7] LIVINGSTON, Dorothy Michelson. *The master of light: a biography of Albert A. Michelson*. New York: Scribner, 1973. ISBN 978-0684134437.

[8] MICHELSON, Albert Abraham a E. W. MORLEY. Influence of motion of the medium on the velocity of light. *America Journal of Science*. 1886, **31**(185), 377–386. DOI: 10.2475/ajs.s3-31.185.377. ISBN 10.2475/ajs.s3-31.185.377. Dostupné z URL: <`http://www.ajsonline.org/cgi/doi/10.2475/ajs.s3-31.185.377`

[9] BORN, Max a Emil WOLF. *Principles of optics: electromagnetic theory of propagation, interference and diffraction of light*. 7th ed. Cambridge: Cambridge University Press, c1999. ISBN 05-216-4222-1.

[10] LACHS, Gerard. *Fiber-optic communications: systems, analysis, and enhancements*. New York: McGraw-Hill, c1998. ISBN 00-703-8279-4.

[11] KUMAR, Shiva a M. Jamal DEEN. *Fiber optic communications: fundamentals and applications*. Chichester, [England]: Wiley, 2014. ISBN 978-1-118-68343-9.

[12] BRACEWELL, Ronald N. *The Fourier transform and its applications*. 2nd ed., rev. New York: McGraw-Hill, c1986. ISBN 00-700-7016-4.

[13] DIENES, Paul. *The Taylor series: An introduction to the theory of functions of a complex variable*. New York: Dover Publications, 1957. ASIN B0006AV7ME.

[14] OKAMOTO, Katsunari. *Fundamentals of optical waveguides*. 2nd ed. Boston: Elsevier, c2006. ISBN 01-252-5096-7.

[15] MARCUSE, Dietrich. *Theory of Dielectric Optical Waveguides*. 2nd. USA: Academic Press, 1991. ISBN 978-0123941855.

[16] FILKA, Miloslav a kol. *Optoelektronika pro telekomunikace a informatiku*. Vyd. 2. Brno: M. Filka, 2017. ISBN 978-80-86785-14-1.

[17] GHAFOURI-SHIRAZ, H. a B. S. K. LO. *Distributed feedback laser diodes: principles and physical modeling*. New York: Wiley, 1996. ISBN 978-0471960058.

[18] MORTHIER, Geert a Patrick. VANKWIKELBERGE. *Handbook of distributed feedback laser diodes*. Second edition. London, United Kingdom: Artech House Publishers, 2013. Artech House applied photonics series. ISBN 978-1608077014.

[19] BOWERS, J. a C. BURRUS. Ultrawide-band long-wavelength p-i-n photodetectors. *Journal of Lightwave Technology*. 1987, **5**(10), 1339-1350. DOI: 10.1109/JLT.1987.1075419. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/1075419/

[20] BASS, Michael a Virendra N. MAHAJAN. *Handbook of optics*. 3rd ed. New York: McGraw-Hill, c2010. ISBN 978-007-1633-130.

[21] LUCOVSKY, G., R. F. SCHWARZ a R. B. EMMONS. Transit-Time Considerations in p—i—n Diodes. *Journal of Applied Physics*. 1964, **35**(3), 622-. DOI: 10.1063/1.1713426. ISSN 00218979. Dostupné z URL: <http://scitation.aip.org/content/aip/journal/jap/35/3/10.1063/1.1713426

[22] TAROF, L. E. Planar InP/InGaAs avalanche photodiodes with a gain-bandwidth product exceeding 100 GHz. *Optical Fiber Communication*. Washington, D.C: OSA, 1991, , ThO3. DOI: 10.1364/OFC.1991.ThO3. ISBN 1-55752-166-2. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?uri=OFC-1991-ThO3

[23] KUWATSUKA, H., T. MIKAWA, S. MIURA, N. YASUOKA, T. TANAHASHI a O. WADA. An Al/sub x/Ga/sub 1-x/Sb avalanche photodiode with a gain bandwidth product of 90 GHz. *IEEE Photonics Technology Letters*. 1990, **2**(1),

54-55. DOI: 10.1109/68.47041. ISSN 1041-1135. Dostupné z URL: <http://ieeexplore.ieee.org/document/47041/

[24] MIKAWA, T., H. KUWATSUKA, Y. KITO, T. KUMAI, M. MAKIUCHI, S. YAMAZAKI, O. WADA a T. SHIRAI. Flip-chip InGaAs avalanche photodiode with ultra low capacitance and large gain-bandwidth product. *Optical Fiber Communication*. Washington, D.C: OSA, 1991, , ThO2. DOI: 10.1364/OFC.1991.ThO2. ISBN 1-55752-166-2. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?uri=OFC-1991-ThO2

[25] SHIBA, T., E. ISHIMURA, K. TAKAHASHI, H. NAMIZAKI a W. SUSAKI. New approach to the frequency response analysis of an InGaAs avalanche photodiode. *Journal of Lightwave Technology*. 1988, **6**(10), 1502-1506. DOI: 10.1109/50.7908. ISSN 07338724. Dostupné z URL: <http://ieeexplore.ieee.org/document/7908/

[26] BERCHTOLD, K., O. KRUMPHOLZ a J. SURI. Avalanche photodiodes with a gain-bandwidth product of more than 200 GHz. *Applied Physics Letters*. 1975, **26**(10), 585-. DOI: 10.1063/1.87985. ISSN 00036951. Dostupné z URL: <http://scitation.aip.org/content/aip/journal/apl/26/10/10.1063/1.87985

[27] OSAKA, F., T. MIKAWA a T. KANEDA. Impact Ionization of Electrons and Holes in (100)-Oriented Ga1 – xInxAsyP1-y. *IEEE J . Quantum Electron*. 1985, **no. 9**(vol . QE-21), 1326–1338.

[28] LEE, C. A., R. A. LOGAN, R. L. BATDORF, J. J. KLEIMACK a W. WIEGMANN. Ionization Rates of Holes and Electrons in Silicon. *Physical Review*. 1964, **134**(3A), A761-A773. DOI: 10.1103/PhysRev.134.A761. ISSN 0031-899x. Dostupné z URL: <http://link.aps.org/doi/10.1103/PhysRev.134.A761

[29] EMMONS, R. B. Avalanche-Photodiode Frequency Response. *Journal of Applied Physics*. 1967, **38**(9), 3705-. DOI: 10.1063/1.1710199. ISSN 00218979. Dostupné z URL: <http://scitation.aip.org/content/aip/journal/jap/38/9/10.1063/1.1710199

[30] MILLER, S. L. Avalanche Breakdown in Germanium. *Physical Review*. 1955, **99**(4), 1234-1241. DOI: 10.1103/PhysRev.99.1234. ISSN 0031-899x. Dostupné z URL: <http://link.aps.org/doi/10.1103/PhysRev.99.1234

[31] MCINTYRE, R.J. Multiplication noise in uniform avalanche diodes. *IEEE Transactions on Electron Devices*. 1966, **ED-13**(1), 164-168. DOI: 10.1109/T-ED.1966.15651. ISSN 0018-9383. Dostupné z URL: <http://ieeexplore.ieee.org/document/1474241/

[32] BRAIN, M. a Tien-pei LEE. Optical receivers for lightwave communication systems. *IEEE Transactions on Electron Devices*. 1985, **32**(12), 2673-2692. DOI: 10.1109/T-ED.1985.22399. ISSN 0018-9383. Dostupné z URL: <http://ieeexplore.ieee.org/document/1485145/

[33] KASPER, B. a J. CAMPBELL. Multigigabit-per-second avalanche photodiode lightwave receivers. *Journal of Lightwave Technology*. 1987, **5**(10), 1351-1364. DOI: 10.1109/JLT.1987.1075425. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/1075425/

[34] MUOI, T. Receiver design for high-speed optical-fiber systems. *Journal of Lightwave Technology*. 1984, **2**(3), 243-267. DOI: 10.1109/JLT.1984.1073617. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/1073617/

[35] NAKAMURA, Hirotaka. [Tutorial]: NG-PON2 technologies. In: *Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC), 2013*. USA: IEEE, 2013, s. 1–52.

[36] *G.984.2 : Gigabit-capable Passive Optical Networks (G-PON): Physical Media Dependent (PMD) layer specification* [online]. Švýcarsko: International Telecommunication Union, 2003 [cit. 2017-03-07]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.984.2

[37] HORVÁTH, Tomáš, Lukáš KOČÍ, Michal JURČÍK a Miloslav FILKA. Coexistence GPON, NG-PON, and CATV systems. *International Journal of Engineering Trends and Technology*. 2015, **21**(2), 61–66. ISSN 2231- 5381.

[38] MULLEROVA, Jarmila, Dusan KORCEK a Milan DADO. On wavelength blocking for XG-PON coexistence with GPON and WDM-PON networks. In: *2012 14th International Conference on Transparent Optical Networks (ICTON)*. Velká Británie: IEEE, 2012, s. 1-4. DOI: 10.1109/ICTON.2012.6253748. ISBN 978-1-4673-2229-4. Dostupné z URL: <http://ieeexplore.ieee.org/document/6253748/

[39] KAUR, Amandeep, M.L. SINGH a Anu SHEETAL. Comparison of RZ and NRZ data formats for co-existing GPON and XG-PON system. In: *International Conference on Advanced Nanomaterials*. Indie: IEEE, 2013, s. 666-669. DOI: 10.1109/ICANMEET.2013.6609379. ISBN 978-1-4799-1379-4. Dostupné z URL: <http://ieeexplore.ieee.org/document/6609379/

[40] *G.987.2 : 10-Gigabit-capable passive optical networks (XG-PON): Physical media dependent (PMD) layer specification* [online]. Švýcarsko: International Telecommunication Union, 2016 [cit. 2017-03-07]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.987.2

[41] EFFENBERGER, Frank. XG-PON1 versus NG-PON2: Which One Will Win? In: *European Conference and Exhibition on Optical Communication*. Washington, D.C: OSA, 2012, Tu.4.B.1-. DOI: 10.1364/ECEOC.2012.Tu.4.B.1. ISBN 978-1-55752-950-3. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?uri=ECEOC-2012-Tu.4.B.1

[42] CHOW, C. W. a C. H. YEH. Technology advances for the 2nd stage next-generation passive-optical-network (NG-PON2). In: *2013 6th IEEE/International Conference on Advanced Infocomm Technology (ICAIT)*. Taiwan: IEEE, 2013, s. 83-84. DOI: 10.1109/ICAIT.2013.6621496. ISBN 978-1-4799-0465-5. Dostupné z URL: <http://ieeexplore.ieee.org/document/6621496/

[43] *G.989.1 : 40-Gigabit-capable passive optical networks (NG-PON2): General requirements* [online]. Švýcarsko: International Telecommunication Union, 2013 [cit. 2017-03-07]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.989.1

[44] LUO, Yuanqiu, Xiaoping ZHOU, Frank EFFENBERGER, Xuejin YAN, Guikai PENG, Yinbo QIAN a Yiran MA. Time- and Wavelength-Division Multiplexed Passive Optical Network (TWDM-PON) for Next-Generation PON Stage 2 (NG-PON2). *Journal of Lightwave Technology*. 2013, **31**(4), 587-593. DOI: 10.1109/JLT.2012.2215841. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/6289432/

[45] *G.989.2 : 40-Gigabit-capable passive optical networks (NG-PON2): Physical media dependent (PMD) layer specification* [online]. Švýcarsko: International Telecommunication Union, 2014 [cit. 2017-03-07]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.989.2

[46] *Digitální Česko v. 2.0: Cesta k digitální ekonomice* [online]. Česká republika: Úřad vlády České republiky, 2012 [cit. 2017-03-07]. Dostupné z URL: <https://www.vlada.cz/assets/media-centrum/aktualne/Digitalni-Cesko-v--2-0_120320.pdf

[47] *Poskytnutí informace - dokumentu Národní plán rozvoje sítí nové generace: (Strategie skokové změny 2030)* [online]. Česká republika: Ministerstvo vnitra

České republiky, 2015 [cit. 2017-03-07]. Dostupné z URL: <https://goo.gl/LXsHGs

[48] *Y.2001 : General overview of NGN* [online]. Švýcarsko: International Telecommunication Union, 2004 [cit. 2017-03-07]. Dostupné z URL: <https://www.itu.int/rec/T-REC-Y.2001/en

[49] *Výroční zpráva Českého telekomunikačního úřadu za rok 2014* [online]. Česká republika: Český telekomunikační úřad, 2015 [cit. 2017-03-07]. Dostupné z URL: <http://www.ctu.cz/vyrocni-zpravy-rok-2014

[50] *Výroční zpráva Českého telekomunikačního úřadu za rok 2015* [online]. Česká republika: Český telekomunikační úřad, 2016 [cit. 2017-03-07]. Dostupné z URL: <http://www.ctu.cz/vyrocni-zpravy-rok-2015

[51] *Národní plán rozvoje sítí nové generace: (pracovní verze ze dne – 5. srpna 2016)* [online]. Česká republika: Ministerstvo průmyslu a obchodu, 2016 [cit. 2017-03-07]. Dostupné z URL: <http://www.mpo.cz/

[52] HORVÁTH, Tomáš, Petr MÜNSTER a Miloslav FILKA. Security Issues in NGA networks. *In: 27th Conference and Exhibition on OPTICAL COMMUNICATIONS 2015, NGA: WITH OR WITHOUT OPTICAL FIBRE*. Praha: Agentura Action M, 2015, s. 34–37. ISBN 978-80-86742-41-0.

[53] *G.984.3 : Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification* [online]. Švýcarsko: International Telecommunication Union, 2014 [cit. 2017-03-07]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.984.3

[54] TRUONG QUANG VINH, JU-HYUN PARK, YOUNG-CHUL KIM a KWANG-OK KIM. An FPGA implementation of 30Gbps security module for GPON systems. In: *2008 8th IEEE International Conference on Computer and Information Technology*. Sydney: IEEE, 2008, s. 868–872. DOI: 10.1109/CIT.2008.4594788. ISBN 978-1-4244-2357-6. Dostupné z URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4594788

[55] *G.988 : ONU management and control interface (OMCI) specification* [online]. Švýcarsko: International Telecommunication Union, 2012 [cit. 2017-03-07]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.988/en

[56] OISHI, Masayuki, Yukio HORIUCHI a Kosuke NISHIMURA. ONU tester for diagnosis of TDMA-PON using multi-point control protocol messages. In: *The*

10th International Conference on Optical Internet (COIN2012). Yokohama: IEEE, 2012, s. 81–82. ISBN 978-1-4673-1654-5. ISSN 2159-6395.

[57] *G.Sup49 : Rogue optical network unit (ONU) considerations* [online]. Švýcarsko: International Telecommunication Union, 2011 [cit. 2017-03-07]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.Sup49-201102-I

[58] DRAKULIC, Sanda, Massimo TORNATORE a Giacomo VERTICALE. Degradation attacks on Passive Optical Networks. In: *2012 16th International Conference on Optical Network Design and Modelling (ONDM)*. Colchester, United Kingdom: IEEE, 2012, s. 1–6. DOI: 10.1109/ONDM.2012.6210184. ISBN 978-1-4673-1442-8. Dostupné z URL: <http://ieeexplore.ieee.org/document/6210184/

[59] HAJDUCZENIA, Marek, Pedro M. INACIO, Henrique DA SILVA, Mario FREIRE a Paulo MONTEIRO. On EPON security issues. *IEEE Communications Surveys*. 2007, **9**(1), 68–83. DOI: 10.1109/COMST.2007.358972. ISSN 1553-877x. Dostupné z URL: <http://ieeexplore.ieee.org/document/4198187/

[60] MENDONCA, Claudia, Mario LIMA a Antonio TEIXEIRA. Security issues due to reflection in PON physical medium. In: *2012 14th International Conference on Transparent Optical Networks (ICTON)*. Coventry, United Kingdom: IEEE, 2012, s. 1–4. DOI: 10.1109/ICTON.2012.6254487. ISBN 978-1-4673-2229-4. Dostupné z URL: <http://ieeexplore.ieee.org/document/6254487/

[61] CHEN, Xianghua, Guochu SHOU, Zhigang GUO a Yihong HU. Encryption and Authentication Mechanism of 10G EPON Systems Based on GCM. In: *2010 2nd International Conference on E-business and Information System Security*. Wuhan, China: IEEE, 2010, s. 1–4. DOI: 10.1109/EBISS.2010.5473490. ISBN 978-1-4244-5893-6. Dostupné z URL: <http://ieeexplore.ieee.org/document/5473490/

[62] YAN, Y., S. YAMASHITA, S.-H. YEN, P.T. AFSHAR, V. GUDLA, L.G. KAZOVSKY a S.-W. WONG. Invited Paper: Challenges in next-generation optical access networks. *IET Optoelectronics*. 2011, **5**(4), 133–143. DOI: 10.1049/iet-opt.2011.0027. ISSN 1751-8768. Dostupné z URL: <http://digital-library.theiet.org/content/journals/10.1049/iet-opt.2011.0027

[63] MARTINEZ-MATEO, Jesus, Alex CIURANA a Vicente MARTIN. Quantum Key Distribution Based on Selective Post-Processing in Passive Optical Networks. *IEEE Photonics Technology Letters*. 2014, **26**(9), 881-884.

DOI: 10.1109/LPT.2014.2308921. ISSN 1041-1135. Dostupné z URL: <http://ieeexplore.ieee.org/document/6762880/

[64] ALEKSIC, Slavisa, Dominic WINKLER, Gerald FRANZL, Andreas POPPE, Bernhard SCHRENK a Florian HIPP. Quantum key distribution over optical access networks. In: *Proceedings of the 2013 18th European Conference on Network and Optical Communications*. Graz, Austria: IEEE, 2013, s. 11–18. DOI: 10.1109/NOC-OCI.2013.6582861. ISBN 978-1-4673-5823-1. Dostupné z URL: <http://ieeexplore.ieee.org/document/6582861/

[65] FROEHLICH, F.F., C.H. PRICE, T.M. TURPIN a J.A. COOKE. All-Optical Encryption for Links at 10 GBPS and Above. In: *MILCOM 2005 - 2005 IEEE Military Communications Conference*. Atlantic City, NJ: IEEE, 2005, s. 1–7. DOI: 10.1109/MILCOM.2005.1605989. ISBN 0-7803-9393-7. Dostupné z URL: <http://ieeexplore.ieee.org/document/1605989/

[66] YIN, Aihan, Qiang LI a Ming ZHU. Secure authentication scheme for 10Gbit/s Ethernet passive optical networks. *Optik - International Journal for Light and Electron Optics*. 2014, **125**(20), 5947-5951. DOI: 10.1016/j.ijleo.2014.06.089. ISSN 00304026. Dostupné z URL: <http://linkinghub.elsevier.com/retrieve/pii/S0030402614007372

[67] XU, Xiaoling, Guochu SHOU, Zhigang GUO a Yihong HU. Encryption method of next generation PON system. In: *2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT)*. Beijing: IEEE, 2010, s. 384–387. DOI: 10.1109/ICBNMT.2010.5705117. ISBN 978-1-4244-6769-3. Dostupné z URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5705117

[68] HORVÁTH, Tomáš, Petr MÜNSTER a Miloslav FILKA. A Novel Unique Parameter for Increasing of Security in GPON networks. *Journal of Communications Software and Systems*. 2016, 12(2), s. 112–116.

[69] HAO, Feng a Siamak F. SHAHANDASHTI. The SPEKE Protocol Revisited. In: *Security Standardisation Research: First International Conference, SSR 2014*. Londýn: Springer International Publishing, 2014, s. 26. DOI: 10.1007/978-3-319-14054-4_2. ISBN 978-3-319-14053-7. ISSN 0302-9743. Dostupné z URL: <http://link.springer.com/10.1007/978-3-319-14054-4_2

[70] BERNSTEIN, Daniel J. Curve25519: New Diffie-Hellman Speed Records. In: Lecture Notes in Computer Science. USA: Springer Berlin Heidelberg, c2006,

s. 207–228. DOI: 10.1007/11745853_14. ISBN 978-3-540-33851-2. ISSN 0302-9743. Dostupné z URL: <http://link.springer.com/10.1007/11745853_14

[71] YIN, Aihan a Shengkai WANG. A novel encryption scheme based on timestamp in gigabit Ethernet passive optical network using AES-128. In: *Optik - International Journal for Light and Electron Optics*. Frankfurt: Elsevier GmbH, 2014, 125(3), s. 1361–1365. DOI: 10.1016/j.ijleo.2013.08.030. ISSN 00304026. Dostupné z URL: <http://linkinghub.elsevier.com/retrieve/pii/S0030402613012072

[72] YIN, Aihan, Qiang LI a Ming ZHU. Secure authentication scheme for 10Gbit/s Ethernet passive optical networks. Optik - International Journal for Light and Electron Optics. 2014, 125(20), 5947–5951. DOI: 10.1016/j.ijleo.2014.06.089. ISSN 00304026. Dostupné z URL: <http://linkinghub.elsevier.com/retrieve/pii/S0030402614007372

[73] MALINA, Lukas, Petr MUNSTER, Jan HAJNÝ a Tomas HORVATH. Towards Secure Gigabit Passive Optical Networks. In: *Proceedings of SECRYPT 2015*. Francie: Colmar, 2015, s. 349–354. ISBN 978-989-758-117-5.

[74] HORVATH, Tomas, Lukas MALINA a Petr MUNSTER. On security in gigabit passive optical networks. In: *2015 International Workshop on Fiber Optics in Access Network (FOAN)*. Brno: IEEE, 2015, s. 51–55. DOI: 10.1109/FOAN.2015.7320479. ISBN 978-1-4673-7625-9. ISSN 2378-847X. Dostupné z URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7320479

[75] MALINA, Lukas, Tomas HORVATH, Petr MUNSTER a Jan HAJNY. Security solution with signal propagation measurement for Gigabit Passive Optical Networks. *Optik - International Journal for Light and Electron Optics*. 2016, 127(16), 6715-6725. DOI: 10.1016/j.ijleo.2016.04.069. ISSN 00304026. Dostupné z URL: <http://linkinghub.elsevier.com/retrieve/pii/S0030402616303448

[76] YUANQIU LUO, Frank EFFENBERGER a BO GAO. Transmission convergence layer framing in XG-PON1. In: *2009 IEEE Sarnoff Symposium*. New Jersey: IEEE, 2009, s. 1–5. DOI: 10.1109/SARNOF.2009.4850314. ISBN 978-1-4244-3381-0. Dostupné z URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4850314

[77] RAD, Mohammad, Kerim FOULI, Habib FATHALLAH, Leslie RUSCH a Martin MAIER. Passive optical network monitoring: challenges and requirements.

IEEE Communications Magazine. 2011, **49**(2), s45-S52. DOI: 10.1109/MCOM.2011.5706313. ISSN 0163-6804. Dostupné z URL: <http://ieeexplore.ieee.org/document/5706313/

[78] YUKSEL, Kivilcim, Veronique MOEYAERT, Marc WUILPART a Patrice MEGRET. Optical layer monitoring in Passive Optical Networks (PONs): A review. In: *2008 10th Anniversary International Conference on Transparent Optical Networks*. Athens, Greece: IEEE, 2008, s. 92-98. DOI: 10.1109/ICTON.2008.4598379. ISBN 978-1-4244-2625-6. Dostupné z URL: <http://ieeexplore.ieee.org/document/4598379/

[79] EHRHARDT, A., F. ESCHER, L. SCHURER, H.-M. FOISEL, A. TEMPLIN, M. ADAMY a C. GERLACH. PON measurements and monitoring solutions for FTTH networks during deployment and operation. In: *Transparent Optical Networks (ICTON), 2011 13th International Conference on*. Stockholm, Sweden: IEEE, 2011, s. 1–6. DOI: 10.1109/ICTON.2011.5970861. ISBN 978-1-4577-0882-4. ISSN 2161-2064. Dostupné z URL: <http://ieeexplore.ieee.org/document/5970861/

[80] ESMAIL, Maged Abdullah a Habib FATHALLAH. Physical Layer Monitoring Techniques for TDM-Passive Optical Networks: A Survey. *IEEE Communications Surveys*. 2013, **15**(2), 943-958. DOI: 10.1109/SURV.2012.060912.00057. ISSN 1553-877x. Dostupné z URL: <http://ieeexplore.ieee.org/document/6226791/

[81] SMITH, Timothy G., Rodney S. TUCKER, Kerry HINTON a An V. TRAN. Packet delay variance and bandwidth allocation algorithms for extended-reach GPON. In: *2009 14th OptoElectronics and Communications Conference*. Hong Kong, China: IEEE, 2009, s. 1-2. DOI: 10.1109/OECC.2009.5222078. ISBN 978-1-4244-4102-0. Dostupné z URL: <http://ieeexplore.ieee.org/document/5222078/

[82] KYEONG-HWAN DOO, SANG-SOO LEE a WHAN-WOO KIM. Design of a retimed long-reach GPON Extender using FPGA. In: *Digest of the 9th International Conference on Optical Internet (COIN 2010)*. Jeju, Korea (South): IEEE, 2010, s. 1-3. DOI: 10.1109/COIN.2010.5546608. ISBN 978-1-4244-7181-2. Dostupné z URL: <http://ieeexplore.ieee.org/document/5546608/

[83] LOPEZ, Eduardo Tommy, Victor POLO, J. A. LAZARO a Josep PRAT. Layer 2 redesign for Metro-Access next generation PON. In: *2014 16th International Conference on Transparent Optical Networks (ICTON)*. Graz, Aus-

tria: IEEE, 2014, s. 1-4. DOI: 10.1109/ICTON.2014.6876387. ISBN 978-1-4799-5601-2. Dostupné z URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6876387

[84] CUI, Qingpei, Tong YE, Tony T. LEE, Wei GUO a Weisheng HU. Stability and Delay Analysis of EPON Registration Protocol. *IEEE Transactions on Communications*. 2014, **62**(7), 2478–2493. DOI: 10.1109/TCOMM.2014.2325573. ISSN 0090-6778. Dostupné z URL: <http://ieeexplore.ieee.org/document/6818442/

[85] SALIOU, Fabienne, Philippe CHANCLOU, Bernard LANDOUSIES, Naveena GENAY a Claude LE BOUËTTÉ. Extended Reach Access Network Based on Aggregation of the G-PON Traffic. In: *Optical Fiber Communication Conference and National Fiber Optic Engineers Conference*. Washington, D.C: OSA, 2009, NThC2-. DOI: 10.1364/NFOEC.2009.NThC2. ISBN 978-1-55752-865-0. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?uri=NFOEC-2009-NThC2

[86] LEE, K L., J. L. RIDING, A. V. TRAN a R. S. TUCKER. Extended-Reach Gigabit Passive Optical Network for Rural Areas Using Distributed Raman Amplifiers. In: *Optical Fiber Communication Conference and National Fiber Optic Engineers Conference*. Washington, D.C: OSA, 2009, NME3-. DOI: 10.1364/NFOEC.2009.NME3. ISBN 978-1-55752-865-0. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?uri=NFOEC-2009-NME3

[87] MERCIAN, Anu, Michael P. MCGARRY a Martin REISSLEIN. Impact of report message scheduling (RMS) in 1G/10G EPON and GPON. *Optical Switching and Networking*. 2014, **12**, 1-13. DOI: 10.1016/j.osn.2013.11.004. ISSN 15734277. Dostupné z URL: <http://linkinghub.elsevier.com/retrieve/pii/S1573427713001094

[88] ALSHAER, Hamada a Mohamed ALYAFEI. An end-to-end QoS scheme for GPON access networks. In: *2011 IEEE GCC Conference and Exhibition (GCC)*. Dubai, United Arab Emirates: IEEE, 2011, s. 513-516. DOI: 10.1109/IEEEGCC.2011.5752584. ISBN 978-1-61284-118-2. Dostupné z URL: <http://ieeexplore.ieee.org/document/5752584/

[89] AURZADA, Frank, Michael SCHEUTZOW, Martin REISSLEIN, Navid GHAZISAIDI a Martin MAIER. Capacity and Delay Analysis of Next-Generation Passive Optical Networks (NG-PONs). *IEEE Transactions on Communications*. 2011, **59**(5), 1378–1388. DOI: 10.1109/TCOMM.2011.030411.100418. ISSN

0090-6778. Dostupné z URL: <http://ieeexplore.ieee.org/document/5733453/

[90] BONILLA, Mauricio López, Felipe Rudge BARBOSA a Edson MOSCHIM. Techno-economical comparison between GPON and EPON networks. In: *Innovations for Digital Inclusions, 2009. K-IDI 2009. ITU-T Kaleidoscope:*. Mar del Plata, Argentina: ITU, 2009, s. 1–5. ISBN 978-92-61-12891-3.

[91] JAY, Stephan, Karl-Heinz NEUMANN a Thomas PLÜCKEBAUM. Comparing FTTH access networks based on P2P and PMP fibre topologies. *Telecommunications Policy*. 2014, **38**(5-6), 415-425. DOI: 10.1016/j.telpol.2013.04.010. ISSN 03085961. Dostupné z URL: <http://linkinghub.elsevier.com/retrieve/pii/S0308596113000694

[92] TOSI BELEFFI, G.M., A. VALENTI, F. MATERA a D. DEL BUONO. Energy Impact of The Future Fibre Optics Access Networks: Economic Perspectives. In: *2015 Fotonica AEIT Italian Conference on Photonics Technologies*. Italy: Institution of Engineering and Technology, 2015, 4 .-4 . DOI: 10.1049/cp.2015.0115. ISBN 978-1-78561-068-4. Dostupné z URL: <http://digital-library.theiet.org/content/conferences/10.1049/cp.2015.0115

[93] HORVATH, Tomas, Petr MUNSTER, Michal JURCIK, Lukas KOCI a Miloslav FILKA. Timing Measurement and Simulation of the Activation Process in Gigabit Passive Optical Networks. *Optica Applicata*. Polská republika, 2015, 45(4), 459–471. ISSN 0078-5466.

[94] HORVATH, Tomas, Petr MUNSTER, Michal JURCIK a Miloslav FILKA. Novel Algorithm in Activation Process of GPON Network. *JCOMSS – Journal of Communications Software and Systems*. 2015, 11(4), 204–209. ISSN 1845-6421.

[95] HORVATH, Tomas, Petr MUNSTER, Lubos DUBRAVEC a Miloslav FILKA. A Novel Rogue ONU Detection Algorithm for GPON Networks. *Optica Applicata*. 2016, 46(4), 11.

[96] IEEE Public Organizationally Unique Identifier List. *IEEE* [online]. USA: IEEE, 2015 [cit. 2017-06-01]. Dostupné z URL: <http://standards-oui.ieee.org/oui.txt

[97] Internet Assigned Numbers Authority. *Ethernet Numbers: IANA MAC Address Block* [online]. Kalifornie: IANA, 2015 [cit. 2017-06-01]. Dostupné z URL: <http://www.iana.org/assignments/ethernet-numbers/ethernet-numbers.xhtml

[98] REKHTER, Y., B. MOSKOWITZ, D. KARRENBERG a G. J. GROOT. RFC 1918: Address Allocation for Private Internets. In: *Internet Engineering Task Force* [online]. Kalifornie, 2015 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc1918

[99] VENAAS, Stig. IPv4 Multicast Address Space Registry. In: *Internet Engineering Task Force* [online]. Kalifornie, 2016 [cit. 2017-06-01]. Dostupné z URL: <https://www.ietf.org/assignments/multicast-addresses/multicast-addresses.txt

[100] FENNER, W. RFC 2236 – Internet Group Management Protocol, Version 2. In: *Internet Engineering Task Force* [online]. Kalifornie, 1997 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc2236

[101] FULLER, V., T. LI, J. YU a K. VARADHAN. RFC 1338: Supernetting: an Address Assignment and Aggregation Strategy. In: *Internet Engineering Task Force* [online]. Kalifornie, 1992 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc1338

[102] ABOBA, B., D. THALER a L. ESIBOV. RFC 4795 – Link-local Multicast Name Resolution (LLMNR). In: *Internet Engineering Task Force* [online]. Kalifornie, 2007 [cit. 2016-08-20]. Dostupné z URL: <https://tools.ietf.org/html/rfc4795

[103] MEYER, D. RFC 2365: Administratively Scoped IP Multicast. In: *Internet Engineering Task Force* [online]. Kalifornie, 1998 [cit. 2017-06-01]. Dostupné z URL: <https://www.ietf.org/rfc/rfc2365.txt

[104] KATZ, D. RFC 2113: IP Router Alert Option. In: *Internet Engineering Task Force* [online]. Kalifornie, 1997 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc2113

[105] BRADEN, R., L. ZHANG, S. BERSON, S. HERZOG a S. JAMIN. RFC 2205 – Resource ReSerVation Protocol (RSVP). In: *Internet Engineering Task Force* [online]. Kalifornie, 1997 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc2205

[106] VENAAS, Stig. IPv6 Multicast Address Space Registry. In: *Internet Assigned Numbers Authority* [online]. Kalifornie: IANA, 2016 [cit. 2017-06-01]. Dostupné z URL: <http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

[107] PERKINS, C. RFC 2003 – IP Encapsulation within IP. In: *Internet Assigned Numbers Authority* [online]. Kalifornie, 1996 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc2003

[108] VIDA, R. a L. COSTA. RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6. In: *Internet Assigned Numbers Authority* [online]. Kalifornie, 2004 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc3810

[109] CHESHIRE, S. a M. KROCHMAL. RFC 6886 – NAT Port Mapping Protocol (NAT-PMP). In: *Internet Assigned Numbers Authority* [online]. Kalifornie, 2013 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc6886

[110] DROMS, R., J. BOUND, B. VOLZ, T. LEMON, C. PERKINS a M. CARNEY. RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). In: Internet Engineering Task Force [online]. Kalifornie, 2003 [cit. 2017-06-01]. Dostupné z URL: <https://tools.ietf.org/html/rfc3315

[111] HORVATH, Tomas, Radko KRKOS a Lubos DUBRAVEC. Deep Data Analysis in GPON Networks. *Optica Applicata*. 0078-5466, 2017, **47**(1), 157–170. ISSN 0078-5466.

[112] MÜNSTER, Petr, Radim ŠIFTA, Tomáš HORVÁTH, Vít NOVOTNÝ a Miloslav FILKA. Fourth Forum of Young Researchers. In *the framework of International Forum Education Quality – 2014. In: Fourth Forum of Young Researchers*. In the framework of International Forum Education Quality – 2014. Izhevsk: Russia: Publishing House, 2014, s. 364–367. ISBN 978-5-7526-0649- 6.

[113] *G.987.3 : 10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification* [online]. Švýcarsko: International Telecommunication Union, 2014 [cit. 2017-06-01]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.987.3

[114] HOOD, Dave a Elmar TROJER. *Gigabit-capable passive optical networks*. Hoboken: Wiley, 2011. ISBN 978-047-0936-870.

[115] BINH, Le Nguyen. *Guided wave photonics: fundamentals and applications with MATLAB*. Boca Raton, FL: CRC Press, c2012. Optics and photonics (Boca Raton, Fla.), 5. ISBN 978-143-9828-557.

[116] KOCI, Lukas, Tomas HORVATH, Petr MUNSTER, Michal JURCIK a Miloslav FILKA. Transmission convergence layer in XG-PON. In: *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*.

Praha: IEEE, 2015, s. 104–108. DOI: 10.1109/TSP.2015.7296232. ISBN 978-1-4799-8498-5. Dostupné z URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7296232

[117] BAO, Ning-Hai, M. Farhan HABIB, Massimo TORNATORE, Charles U. MARTEL a Biswanath MUKHERJEE. Global Versus Essential Post-Disaster Re-Provisioning in Telecom Mesh Networks. Journal of Optical Communications and Networking. 2015, 7(5), 392–400. DOI: 10.1364/JOCN.7.000392. ISSN 1943-0620. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?URI=jocn-7-5-392

[118] BAO, Ning-Hai, Massimo TORNATORE, Charles U. MARTEL a Biswanath MUKHERJEE. Fairness-Aware Degradation Based Multipath Re-provisioning Strategy for Post-Disaster Telecom Mesh Networks. Journal of Optical Communications and Networking. 2016, 8(6), 441–450. DOI: 10.1364/JOCN.8.000441. ISSN 1943-0620. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?URI=jocn-8-6-441

[119] LIN, Bin, Lin LIN a Pin-Han HO. Cascaded splitter topology optimization in LRPONs. In: *2012 IEEE International Conference on Communications (ICC)*. Ottawa, ON, Canada: IEEE, 2012, s. 3105–3109. DOI: 10.1109/ICC.2012.6364216. ISBN 978-1-4577-2053-6. Dostupné z URL: <http://ieeexplore.ieee.org/document/6364216/

[120] LIN, Lin, Bin LIN a Pin-Han HO. Power-aware optimization modeling for cost-effective LRPON infrastructure deployment. In: *2013 21st International Conference on Software, Telecommunications and Computer Networks - (SoftCOM 2013)*. Split-Primosten, Croatia: IEEE, 2013, s. 1–5. DOI: 10.1109/SoftCOM.2013.6671897. ISBN 978-953-290-040-8. Dostupné z URL: <http://ieeexplore.ieee.org/document/6671897/

[121] CHRISTODOULOU, C., K. MANOUSAKIS a G. ELLINAS. An optimization algorithm for downstream wavelength selection and scheduling in WDM PON-based mobile backhaul networks. In: *2016 18th Mediterranean Electrotechnical Conference (MELECON)*. Lemesos, Cyprus: IEEE, 2016, s. 1–6. DOI: 10.1109/MELCON.2016.7495432. ISBN 978-1-5090-0058-6. Dostupné z URL: <http://ieeexplore.ieee.org/document/7495432/

[122] ARÉVALO, G.V., J.E. SIERRA, R.C. HINCAPIÉ a R. GAUDINO. A novel algorithm for PON optimal deployment over real city maps and large number of users. In: *18th Italian National Conference on Photonic Technologies (Fotonica*

2016). San Pietro, Italy: Institution of Engineering and Technology, 2016, 07 (4 .)-07 (4 .). DOI: 10.1049/cp.2016.0867. ISBN 978-1-78561-268-8. Dostupné z URL: <http://digital-library.theiet.org/content/conferences/10.1049/cp.2016.0867

[123] KANTARCI, Burak a Hussein T. MOUFTAH. Periodic GATE Optimization (PGO): A New Service Scheme for Long-Reach Passive Optical Networks. *IEEE Systems Journal*. 2010, **4**(4), 440–448. DOI: 10.1109/JSYST.2010.2082070. ISSN 1932-8184. Dostupné z URL: <http://ieeexplore.ieee.org/document/5635431/

[124] OKI, Eiji. Linear programming and algorithms for communication networks a practical guide to network design, control, and management. Boca Raton: CRC Press, 2013. ISBN 978-146-6552-647.

[125] FOURER, Robert., David M. GAY a Brian W. KERNIGHAN. AMPL: a modeling language for mathematical programming. 2nd ed. Pacific Grove, CA: Thomson/Brooks/Cole, c2003. ISBN 05-343-8809-4.

[126] IRELAND, Phil, Rod CASE, John FALLIS, Carl Van DYKE, Jason KUEHN a Marc MEKETON. The Canadian Pacific Railway Transforms Operations by Using Models to Develop Its Operating Plans. Interfaces. 2004, 34(1), 5-14. DOI: 10.1287/inte.1030.0055. ISSN 0092-2102. Dostupné z URL: <http://pubsonline.informs.org/doi/abs/10.1287/inte.1030.0055

[127] Cisco. *The Zettabyte Era—Trends and Analysis* [online]. San Jose, USA: Cisco, 2016 [cit. 2017-06-01]. Dostupné z URL: <http://goo.gl/dAO7EY

[128] WANG, Rui, Partha BHAUMIK, Han Hyub LEE, Sang Soo LEE a Biswanath MUKHERJEE. Energy Management in NG-PON2. In: *Optical Fiber Communication Conference*. Washington, D.C: OSA, 2014, Tu3C.4-. DOI: 10.1364/OFC.2014.Tu3C.4. ISBN 978-1-55752-993-0. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?uri=OFC-2014-Tu3C.4

[129] BERTIGNONO, Luca, Stefano CAPRIATA, Valter FERRERO, Laura GREBORIO, Roberto MERCINELLI, Maurizio VALVO a Roberto GAUDINO. Photon ranging techniques for upstream signalling in TWDM-PON during ONU activation. In: *2015 European Conference on Optical Communication (ECOC)*. Valencia, Spain: IEEE, 2015, s. 1-3. DOI: 10.1109/ECOC.2015.7341827. ISBN 978-8-4608-1741-3. Dostupné z URL: <http://ieeexplore.ieee.org/document/7341827/

[130] LUO, Yuanqiu, Bo GAO, Ming JIANG a Frank EFFENBERGER. N:1 fast protection in NG-PON2. In: *2015 Opto-Electronics and Communications Conference (OECC)*. Shanghai, China: IEEE, 2015, s. 1–3. DOI: 10.1109/OECC.2015.7340071. ISBN 978-1-4673-7944-1. Dostupné z URL: <http://ieeexplore.ieee.org/document/7340071/

[131] GROBE, Klaus. WDM-PON with Wavelength-Routed ODN – Pros'n'Cons. In: *Photonic Networks; 16. ITG Symposium; Proceedings of*. Germany: VDE, 2015, s. 51–57. ISBN 978-3-8007-3938-7.

[132] MATSUI, Yasuhiro, Wen LI, Hal ROBERTS, Henk BULTHUIS, Hongyu DENG, Leo LIN a Charles ROXLO. Transceiver for NG-PON2: Wavelengtth Tunablity for Burst Mode TWDM and Point-to-point WDM. In: *Optical Fiber Communication Conference*. Washington, D.C: OSA, 2016, Tu2C.1-. DOI: 10.1364/OFC.2016.Tu2C.1. ISBN 978-1-943580-07-1. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?URI=OFC-2016-Tu2C.1

[133] HATTORI, Kyota, Masahiro NAKAGAWA, Toshiya MATSUDA, Masaru KATAYAMA a Katsutoshi KODA. Passive Optical Metro Network based on NG-PON2 with Sharing Burst-mode Receiver between Continuous-mode and Burst-mode Transmitters to Support Cloud. In: *ECOC 2016; 42nd European Conference on Optical Communication*. Düsseldorf, Germany: VDE, 2016, s. 902–904. ISBN 978-3-8007-4274-5.

[134] LUO, Yuanqiu, Hal ROBERTS, Klaus GROBE, et al. Physical Layer Aspects of NG-PON2 Standards—Part 2: System Design and Technology Feasibility [Invited]. *Journal of Optical Communications and Networking*. 2016, **8**(1), 43-. DOI: 10.1364/JOCN.8.000043. ISSN 1943-0620. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?URI=jocn-8-1-43

[135] NESSET, Derek. NG-PON2 Technology and Standards. *Journal of Lightwave Technology*. 2015-3-1, **33**(5), 1136–1143. DOI: 10.1109/JLT.2015.2389115. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/7005437/

[136] KHOTIMSKY, Denis A. NG-PON2 Transmission Convergence Layer: A Tutorial. *Journal of Lightwave Technology*. 2016-3-1, **34**(5), 1424-1432. DOI: 10.1109/JLT.2016.2523343. ISSN 0733-8724. Dostupné z URL: <http://ieeexplore.ieee.org/document/7394098/

[137] NESSET, Derek. PON Roadmap [Invited]. *Journal of Optical Communications and Networking*. 2017, **9**(1), A71-. DOI: 10.1364/JOCN.9.000A71. ISSN

1943-0620. Dostupné z URL: <https://www.osapublishing.org/abstract.cfm?URI=jocn-9-1-A71

[138] HORVATH, Tomas, Petr MUNSTER, Josef VOJTECH, Ondrej HAVLIS a Martin GALLO. Transmission Convergence Layer of NG-PON2 in VPIphotonics Tool. *Journal of Communications Software and Systems*. 2017, , 1–7. ISSN 1845-6421.

SEZNAM ZKRATEK

10G-EPON	10G EPON – 10G EPON síť
3DEA	Triple DES Algorithm – bloková šifra založená na šifrování DES
ADSL	Asymmetric Digital Subscriber Line – asymetrická digitální linka
AES	Advanced Encryption Standard – standard pokročilého šifrování
APD	Avalanche Photodiode – lavinová dioda
API	Application Programming Interface – rozhraní pro programování aplikací
ARP	Address Resolution Protocol – služební protokol pro překlad adres
BCH	Bose-Chaudhury-Hocquengham – cyklický zabezpečovací kód
BER	Bit Error Rate – bitová chybovost
BPON	Broadband PON – širokopásmová pasivní optická síť
BOTDR	Brillouin Optical Time Domain Relflectometry – Brillouinova reflektometrická měřicí metoda
BWmap	Bandwidth Map – informace o počtu přidělených časových slotů pro ONU
CMD	Command Line – příkazový řádek
CO	Central Office – centrální ústředí poskytovatele
CPU	Central Processor Unit – centrální procesorová jednotka
CSMA	Carrier Sense Multiple Access – metoda mnohonásobného přístupu k médiu
CW	Continuous Wave – kontinuální vlna
ČTÚ	Český telekomunikační úřad
DBA	Dynamic Bandwidth Algorithm – algoritmus pro dynamické přidělení šířky pásma
DBR	Distributed Bragg Reflector – laser s Braggovskými zrcadly

DES	Digital Data Encryption Standard – standard pro zabezpečení přenášených dat
DFB	Distributed FeedBack – laser s rozloženou zpětnou vazbou
DHCPv6	Dynamic Host Configuration Protocol v6 – protokol pro automatickou konfiguraci zařízení v síti pod IPv6
DNS	Domain Name System – systém doménovým jmen
DoS	Denial of Service – odepření služby
EAPoL	Extensible Authentication Protocol over Local Area Network – rozšířený autentizační protokol
ECDH	Elliptic Curve Diffie–Hellman – Diffieho-Hellmanův protokol s využitím eliptických křivek
ENF	Excess Noise Factor – statistický šum
EPON	Ethernet PON – pasivní optická síť založená na přenosu Ethernet rámců
FBG	Fiber Bragg Grating – Bragovy mřížky
FEC	Forward Error Correction – dopředná korekce chyb
FER	Frame Error Rate – chybovost rámců
FPGA	Field-Programmable Gate Array – programovatelná hradlová pole
FS	Framing Sublayer – rámcová podvrstva/rámec této vrstvy
FTTA	Fiber to the Antenna – optické vlákno k anténě
FTTB	Fiber to the Building – optické vlákno do budovy
FTTC	Fiber to the Curb – optické vlákno k obrubníku
FTTH	Fiber to the Home – optické vlákno do bytu
FTTN	Fiber to the Node – optické vlákno do distribučního uzlu
FTTO	Fiber to the Office – optické vlákno do kanceláře
FTTx	Fiber to the ... – optické vlákno do ...

GBP	Gain-Bandwidth Product – součin šířky pásma a k ní příslušejícího zesílení
GEM	Gigabit-capable passive optical network Encapsulation Method – zapouzdřovací metoda pro GPON sítě
GPON	Gigabit Passive Optical Network – gigabitová pasivní optická síť
GTC	Gigabit Passive Optical Network Transmission Convergence – přenosová vrstva GPON sítí
HMAC	Keyed-Hash Message Authentication Code – typ autentizačního kódu zprávy
HEC	Hybrid Error Correction – hybridní korekce chyb
ICMP	Internet Control Message Protocol – protokol pro diagnostiku sítí
IGMP	Internet Group Message Protocol – protokol pro skupinová vysílání
IEEE	Institute of Electrical and Electronics Engineers – institut pro elektrotechnické a elektronické inženýrství
ILP	Integer Linear Programming – celočíselné programování
IP	Internet Protocol – internetový protokol
IPv4	Internet Protocol version 4 – internetový protokol verze 4
IPv6	Internet Protocol version 6 – internetový protokol verze 6
ISO/OSI	International Organization for Standardization/Open Systems Interconnection – sedmi-vrstvý referenční model ISO/OSI
ISP	Internet Service Provider – poskytovatel připojení k Internetu
ITU	International Telecommunication Union – Mezinárodní telekomunikační unie
KDF	Key Derivation Function – funkce odvození klíče
LAN	Local Area Network – lokální síť
LODS	Loss of Downstream – ztráta synchronizace v sestupném směru
LOS	Loss of Signal – ztráta signálu
LOF	Loss of Frame – ztráta rámce

LSB	Low Significant Bit – nejméně významný bit
MAC	Media Access Control – identifikátor síťového zařízení
MILP	Mixed Integer Linear Programming – lineární programování včetně desetinných čísel
NATPMP	Network Adress Translation Port Mapping Protocol – protokol překladu adres
NGN	Next Generation Networks – sítě nové generace
N(X)G-PON	Next Generation PON – pasivní optická síť další generace
NG-PON2	Next Generation PON Stage 2 – pasivní optická síť druhé generace
NRZ	Non Return Zero – linkový kód bez návratu k nule
OAM	Operation, Administration and Maintenance – komunikace procesů, administrace a údržby
ODN	Optical Distribution Network – optická distribuční síť
OLT	Optical Line Termination – optické linkové zakončení
OMCC	Optical Network Unit Management and Control Channel – řídicí a kontrolní kanál v GPON sítích
OMCI	Optical netowrk unit Management and Control Interface – řídicí a kontrolní rozhraní v GPON sítích
ONU	Optical Network Unit – optická síťová jednotka
OTDL	Optical Tapped Delay Line – optická zpožďovací linka
OTDR	Optical Time Domain Relflectometry – reflektometrická měřicí metoda
OUI	Organizationally Unique Identifier – unikátní identifikátor organizace
P2MP	Point to Multipoint – spojení bod-mnohobod
PC	Personal Computer – osobní počítač
PCBd	Physical Control Block downstream – synchronizační blok fyzické vrstvy
PHY	Physical interface – fyzické rozhraní/bitová posloupnost na tomto rozhraní

PIN	Positive-Intrinsic-Negative – fotodioda s velkou neutrálně dopovanou vrstvou mezi p-dopovanými a n-dopovanými oblastmi polovodiče
PLOAM	Physical Layer OAM Operations, Administrations and Maintenance – správa fyzické vrstvy
PLOu	Physical Layer oVERHEAD UPSTREAM – synchronizační část zprávy ve vzestupném směru
PMD	Polarization Mode Dispersion – polarizačně vidová disperze
PSBd	Physical Synchronization Block downstream – synchronizační blok v sestupném směru
PSync	Physical Synchronization – synchronizace sestupného směru
QoS	Quality of Service – kvalita služby
RAM	Random Access Memory – paměť s náhodným přístupem
RTT	Round Trip Time – obousměrné zpoždění
SFC	Super Frame Counter – počítadlo superrámců
RWA	Routing and Wavelength Assignment – problematika směrování a přiřazování vlnových délek
SFP	Small Form-factor Pluggable – zásuvný SFP modul
SFP+	Small Form-factor Pluggable Plus – zásuvný SFP modul s rychlostí 10 Gbit/s
SHA-2	Secure Hash Algorithm – rozšířená hashovací funkce
SPEKE	Simple Password Exponential Key Exchange – metoda ustanovení klíče s využitím modulárního umocňování a sdíleného hesla
T-CONT	Transmission Container – přenosový kontejner dat v GPON sítích
TCP	Transmission Control Protocol – spojově orientovaný protokol
TDM	Time Division Multiplex – časově dělený multiplex
TWDM-PON	Time Wavelength Division Multiplexing PON – pasivní optická síť na principu časového a vlnového multiplexu
UDP	User Datagram Protocol – spojově neorientovaný protokol

VLANID	Virtual Local Area Network Identificator – identifikátor virtuální lokální sítě
WDM	Wavelength Division Multiplexing – vlnově dělený multiplex
XGEM	XG-PON Encapsulation Method – zapouzdřovací metoda sítí nové generace

PUBLIKAČNÍ ČINNOST AUTORA

Články v impaktovaném periodiku:

MUNSTER, Petr, Tomas HORVATH, Ondrej HAVLIS, Martin SLAPAK, Pavel SKODA, Jan RADIL, Radek VELC a Miloslav HULA. Interference of Data Transmission in Access and Backbone Networks by High-Power Sensor System. *Fiber and Integrated Optics*. 2017, , 144–156. DOI: 10.1080/01468030.2017.1327624.

VOJTECH, Josef, Martin SLAPAK, Pavel SKODA, Jan RADIL, Ondrej HAVLIS, Michal ALTMANN, Petr MUNSTER, Radek VELC, Jan KUNDRAT, Lada ALTMANNOVA, Rudolf VOHNOUT, Tomas HORVATH, et al. Joint accurate time and stable frequency distribution infrastructure sharing fiber footprint with research network. *Optical Engineering*. 2017, **56**(2), 027101-. DOI: 10.1117/1.OE.56.2.027101. ISSN 0091-3286.

HORVATH, Tomas, Radko KRKOS a Lubos DUBRAVEC. Deep data analysis in gigabit passive optical networks. *Optica Applicata*. 2017, **47**(1), 157–170.

HORVATH, Tomas, Petr MUNSTER, Lubos DUBRAVEC a Miloslav FILKA. Novel rogue optical network unit detection algorithm for gigabit passive optical networks. *Optica Applicata*. 2016, **46**(3), 421–433.

MALINA, Lukas, Tomas HORVATH, Petr MUNSTER a Jan HAJNY. Security solution with signal propagation measurement for Gigabit Passive Optical Networks. *Optik - International Journal for Light and Electron Optics*. 2016, **127**(16), 6715-6725. DOI: 10.1016/j.ijleo.2016.04.069. ISSN 00304026.

HORVATH, Tomas, Petr MUNSTER, Michal JURCIK, Lukas KOCI a Miloslav FILKA. Timing measurement and simulation of the activation process in gigabit passive optical networks. *Optica Applicata*. 2015, **45**(4), 459–470.

SIFTA, Radim, Petr MUNSTER, Petr SYSEL, Tomas HORVATH, Vit NOVOTNY, Ondrej KRAJSA a Miloslav FILKA. Distributed Fiber-Optic Sensor for Detection and Localization of Acoustic Vibrations. *Metrology and Measurement Systems*. 2015-01-1, **22**(1), 111–118. DOI: 10.1515/mms-2015-0009. ISSN 2300-1941.

Články v odborném periodiku (SCOPUS):

HORVATH, Tomas, Petr MUNSTER, Josef VOJTECH a Ondrej HAVLIS. Modified GIANT Dynamic Bandwidth Allocation Algorithm of NG-PON. *Journal of Communications Software and Systems*. 2017, **13**(1), 15–22. DOI: 10.24138/jcomss.v13i1.243. ISSN 1846-6079.

CUCKA, Milan, Petr MUNSTER, Lukas KOCI, Tomas HORVATH, Miloslav FILKA a Josef VOJTECH. Transmission of High Power Sensor System and DWDM

Data System in One Optical Fiber. *Journal of Communications Software and Systems*. 2016, **12**(4), 190-194. DOI: 10.24138/jcomss.v12i4.77. ISSN 18456421.

HORVATH, Tomas, Petr MUNSTER a Miloslav FILKA. A Novel Unique Parameter for Increasing of Security in GPON Networks. *Journal of Communications Software and Systems*. 2016, **12**(2), 112–116. DOI: 10.24138/jcomss.v12i2.82. ISSN 1846-6079.

JURCIK, Michal a Tomas HORVATH. Visualization Tool for Control Signalling in NG-PON2. *Journal of Communications Software and Systems*. 2016, **12**(2), 117–121. DOI: 10.24138/jcomss.v12i2.83. ISSN 1846-6079.

KOCI, Lukas, Petr MUNSTER, Tomas HORVATH, Milan CUCKA a Miloslav FILKA. The Influence of Digital Modulations on 320 Gbit/s Optical Time Division Multiplexing. *Journal of Communications Software and Systems*. 2015, **11**(4), 187–191. DOI: 10.24138/jcomss.v11i4.96. ISSN 1846-6079.

HORVATH, Tomas, Petr MUNSTER, Michal JURCIK a Miloslav FILKA. Novel Algorithm in Activation Process of GPON Networks. *Journal of Communications Software and Systems*. 2015, **11**(4), 204–209. DOI: 10.24138/jcomss.v11i4.99. ISSN 1846-6079.

Články v konferenčních sbornících:

MÜNSTER, Petr, Jan RADIL, Josef VOJTECH, Ondrej HAVLIS, Tomas HORVATH, Vladimir SMOTLACHA a Edvin SKALJO. Simultaneous transmission of the high-power phase sensitive OTDR, 100Gbps dual polarisation QPSK, accurate time/frequency, and their mutual interferences. In: *Fiber Optic Sensors and Applications XIV*. USA: SPIE, 2017, 102080D-. DOI: 10.1117/12.2267259. ISBN: 9781510609174.

MÜNSTER, Petr, Tomas HORVATH, Ondrej HAVLIS, Josef VOJTECH, Jan RADIL, Radek VELC a Edvin SKALJO. Simultaneous transmission of standard data, precise time, stable frequency and sensing signals and their possible interaction. In: *Optical Sensors 2017*. SPIE, 2017, 102312A-. DOI: 10.1117/12.2266240. ISBN 9781510609631.

MUNSTER, Petr, Josef VOJTECH, Tomas HORVATH, et al. Coexistence of access and backbone networks with sensor systems. In: *2016 International Workshop on Fiber Optics in Access Network (FOAN)*. Lisbon, Portugal: IEEE, 2016, s. 1–5. DOI: 10.1109/FOAN.2016.7764538. ISBN 978-1-5090-3319-5.

OUJEZSKY, Vaclav a Tomas HORVATH. Case study and comparison of SimPy 3 and OMNeT Simulation. In: *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*. Vienna, Austria: IEEE, 2016, s. 15-19. DOI: 10.1109/TSP.2016.7760821. ISBN 978-1-5090-1288-6.

OUJEZSKY, Vaclav, Tomas HORVATH a Vladislav SKORPIL. Modeling botnet C. In: *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*. Vienna, Austria: IEEE, 2016, s. 50-55. DOI: 10.1109/TSP.2016.7760827. ISBN 978-1-5090-1288-6.

OUJEZSKY, Vaclav a Tomas HORVATH. NetFlow Console Collector– Analyzer Developed in Python Language. In: *International Interdisciplinary PhD Workshop 2016*. Brno: Brno University of Technology, 2016, s. 107–110. ISBN: 9788021453876.

MUNSTER, Petr, Josef VOJTECH, Tomas HORVATH, Ondrej HAVLIS, Pavel HANAK, Milan CUCKA a Miloslav FILKA. Simultaneous transmission of distributed sensors and data signals. In: *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*. Vienna, Austria: IEEE, 2016, s. 761-764. DOI: 10.1109/TSP.2016.7760987. ISBN 978-1-5090-1288-6.

HORVATH, Tomas, Petr MUNSTER a Miloslav FILKA. Security Issues in NGA networks. In: *OK2015 – 27th Conference and Exhibition on OPTICAL COMMUNICATIONS 2015*, Praha: Agentura Action M, 2015, s. 34–37. ISBN 978-80-86742-41-0.

HORVATH, Tomas, Lukas MALINA a Petr MUNSTER. On security in gigabit passive optical networks. In: *2015 International Workshop on Fiber Optics in Access Network (FOAN)*. Brno, Czech Republic: IEEE, 2015, s. 51-55. DOI: 10.1109/FOAN.-2015.7320479. ISBN 978-1-4673-7625-9.

MALINA, Lukas, Petr MUNSTER, Jan HAJNY a Tomas HORVATH. Towards secure Gigabit Passive Optical Networks: Signal propagation based key establishment. In: *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*. Colmar, France: IEEE, 2015, s. 1–6. ISBN 978-989-758-117-5.

MUNSTER, Petr, Josef VOJTECH, Petr SYSEL, Radim SIFTA, Vit NOVOTNY, Tomas HORVATH, Stanislav SIMA a Miloslav FILKA. Φ-OTDR signal amplification. In: *Optical Sensors*. SPIE, 2015, s. 950606-. DOI: 10.1117/12.2179026.

KOCI, Lukas, Tomas HORVATH, Petr MUNSTER, Michal JURCIK a Miloslav FILKA. Transmission convergence layer in XG-PON. In: *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*. Praha: IEEE, 2015, s. 104–108. DOI: 10.1109/TSP.2015.7296232. ISBN 978-1-4799-8498-5.

HORVATH, Tomáš. Triple play služby v sítích XG- PON. In: *Proceedings of the 21st Conference STUDENT EEICT 2015*. Brno: Vysoké učení technické v Brně, 2015, s. 561–566. ISBN 978-80-214-5148-3.

NOVOTNY, Vit, Petr SYSEL, Radim SIFTA, Petr MUNSTER, Tomas HORVATH a Miloslav FILKA. Distributed fiber-optic sensor system based on phase- sensitive OTDR. In: *OPTICAL COMMUNICATIONS 2014*. Praha: Agentura Action M, 2014, s. 20–23. ISBN 978-80-86742-39-7.

MUNSTER, Petr, Radim SIFTA, Tomas HORVATH, Vit NOVOTNY a Miloslav FILKA. Polarization mode dispersion in NG-PON. In: *Fourth Forum of Young Researchers. In the framework of International Forum Education Quality – 2014*. Izhevsk: Russia: Publishing House, 2014, s. 364–367. ISBN 978-5-7526-0649-6.

HORVATH, Tomas, Petr MUNSTER a Radim SIFTA. Simulace Triple Play služeb v sítích NG-PON2. In: *Sborník příspěvků studentské konference Zvůle 2014*. Zvůle, 2014, s. 15–18. ISBN 978-80-214-5005-9.

Články v odborných periodicích:

OUJEZSKY, Vaclav, Tomas HORVATH a Vladislav SKORPIL. Botnet C&C Traffic and Flow Lifespans Using Survival Analysis. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*. 2017, 6(1), 38–44. DOI: 10.11601/ijates.v6i1.205. ISSN 1805-5443.

HORVATH, Tomas, Radek FUJDIAK, Milan CUCKA, Marie DANKOVA a Jiri MISUREC. Comparison of Bit Error Rate of Line Codes in NG-PON2. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*. 2016, 5(2), 95–100. DOI: 10.11601/ijates.v5i2.165. ISSN 1805-5443.

KOCI, Tomas, Lukas KOCI, Michal JURCIK a Miloslav FILKA. Coexistence G-PON, NG-PON, and CATV systems. *International Journal of Engineering Trends and Technology*. 2015, 21(2), 61–66. ISSN 2231-5381.

KOVAC, Filip, Radim SIFTA a Tomas HORVATH. Comparison of PMD measuring methods and their reproducibility. *Elektrorevue*. 2015, 6(3), 11–14. ISSN 1213-1539.

HORVATH, Tomas, Radek FUJDIAK, Milan CUCKA a Jiri MISUREC. Using Miller's Code in NG-PON2 Networks. *Elektrorevue*. 2014, 5(2), 20–25. ISSN 1213-1539.

MUNSTER, Petr, Radim SIFTA a Tomas HORVATH. Dvoustavové modulace v OTDM sítích. *Elektrorevue*. 2013, 15(5), 339–342. ISSN 1213-1539.

SIFTA, Radim, Petr MUNSTER a Tomas HORVATH. Přesnost měření disperzí CD/PMD. *Elektrorevue*. 2013, 15(5), 333–339. ISSN 1213-1539.

HORVATH, Tomas, Radim SIFTA a Petr MUNSTER. Detekce hudebních a komprimovaných souborů v BitTorrent protokolu. *Access Server*. 2013, 11(1), 1–4. ISSN 1214- 9675.

HORVATH, Tomas, Radim SIFTA a Petr MUNSTER. Měření služeb Triple play v pasivních optických sítíc. *Elektrorevue*. 2013, 15(3), 1–12. ISSN 1213-1539.

Vysokoškolská skripta:

HORVATH, Tomas. *Fyzická a přenosová vrstva pasivních optických sítí*. Brno, 2015. Skripta.

Kapitola v knize:

FILKA, Miloslav a kol. *Optoelektronika pro telekomunikace a informatiku*. Vyd. 2. Brno: M. Filka, 2017. ISBN 978-80-86785-14-1.

Články v recenzním řízení:

HORVATH, Tomas, Petr MUNSTER, Josef VOJTECH, Ondrej HAVLIS a Martin GALLO. Transmission Convergence Layer of NG-PON2 in VPIphotonics Tool. *Journal of Communications Software and Systems*. 2017, , 1–7. ISSN 1845-6421. SCOPUS

CURRICULUM VITÆ

Ing. Tomáš Horváth

Osobní údaje

Datum narození:	7. 3. 1989
Místo narození:	Havířov
Národnost:	Česká
Stav:	svobodný
Kontakt:	+420 733 328 274, T.Horvath@seznam.cz

Vzdělání

2013–Současnost	obor: Teleinformatika, Vysoké učení technické v Brně, téma dizertační práce: Optimalizace služeb v optických přístupových sítích FTTx.
2011–2013	obor: Telekomunikační a informační technika, Vysoké učení technické v Brně, téma diplomové práce: Simulace a měření služeb Triple Play v sítích FTTx.
2008–2011	obor: Teleinformatika, Vysoké učení technické v Brně, téma bakalářské práce: Switche pro FTTx – nasazení v sítích s IPTV.

Studijní stáže

2016	Studijní stáž v Číně, Chongqing University of Posts and Telecommunications, No2 Chongwen Road,, Nan'an District, Chongqing 400001, China, People's Republic, školitel: prof. Ning-Hai Bao, Ph.D., délka stáže: 4 měsíce.
2015	Studijní stáž v Číně, Chongqing University of Posts and Telecommunications, No2 Chongwen Road,, Nan'an District, Chongqing 400001, China, People's Republic, školitel: prof. Ning-Hai Bao, Ph.D., délka stáže: 3 měsíce.

Jazykové dovednosti

Český jazyk	Mateřský
Čínština	A2
Anglický jazyk	Úroveň B1

Profesní zkušenosti

2016–Současnost	Zaměstnanec, CESNET z. s. p. o.
2015–Současnost	Zaměstnanec, Ústav Telekomunikací, VUT v Brně.
2013	Vědecko-výzkumný pracovník centra SIX, VUT v Brně.
2013	Správce sítě, Elektromotory Vlastimil Moravec.

Certifikace a významné kurzy

Odborné	Kurzy CISCO Akademie (CCNA1/CCNA4)+(CCNP1/CCNP2) VUT. Základy vědecké práce, Akademie věd ČR (Brno).
Měkké znalosti	Příprava prezentací v Prezi 1+2, Efektivní vyjednávání I., Google Analytics, Typografická pravidla, Typografická pravidla v praxi, Kurz projektového řízení pro zaměstnance; ICV (Brno).

Výzkumné aktivity

2017–Současnost	E-infrastruktura CESNET – modernizace. Role v projektu: člen řešitelského týmu.
2017–Současnost	VI20172019072: Detekce bezpečnostních hrozeb na aktivních prvcích kritických infrastruktur. Poskytovatel: Ministerstvo vnitra ČR. Role v projektu: člen řešitelského týmu.
2017–Současnost	VI20172020110: Redukce bezpečnostních hrozeb v optických sítích. Poskytovatel: Ministerstvo vnitra ČR. Role v projektu: člen řešitelského týmu.
2017–Současnost	FEKT-S-17-4184: Výzkum informačních a komunikačních systémů a jejich bezpečnost. Role v projektu: člen řešitelského týmu.
2015–Současnost	VI20152020045: Detekce ohrožení bezpečnosti infrastruktur. Poskytovatel: Ministerstvo vnitra ČR. Role v projektu: člen řešitelského týmu.
2014–2016	FEKT-S-14-2352: Výzkum elektronických a informačních systémů. Role v projektu: člen řešitelského týmu.
2013	CZ.1.05/2.1.00/03.0072: Centrum senzorických, informačních a komunikačních systémů (300 mil. Kč), poskytovatel: Operační program pro vědu a výzkum pro inovace.

Určený recenzent

- 9th International Multi-Conference on Engineering and Technological Innovation.
- IJATES – Internet All-Electronic Journal, ISSN 1805-5443.
- Optica Applicata, ISSN 0078-5466.
- IEEE Communications Surveys & Tutorials, ISSN: 1553-877X.
- Technologická agentura České republiky.

Publikace v číslech

Články v odborném impaktovaném periodiku: 7
Články v odborném SCOPUS periodiku: 6
Články v jiném odborném periodiku: 9
Články publikované na mezinárodních konferencích: 11
Články publikované na domácích konferencích: 4
Články v indexované v databázi WoS: 13
Vysokoškolská skripta: 1
Kapitola v knize: 1
H-index podle databáze WoS: 2

Poslední aktualizace dne **12. 6. 2017**