VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

**FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ**

ÚSTAV TELEKOMUNIKACÍ

Ing. Tomáš Horváth

OPTIMALIZACE SLUŽEB V OPTICKÝCH PŘÍSTUPOVÝCH SÍTÍCH FTTX

SERVICES OPTIMIZATION IN FTTX OPTICAL ACCESS NETWORKS

ZKRÁCENÁ VERZE PH.D. THESIS

Obor: Teleinformatika
Školitel: prof. Ing. Miloslav Filka, CSc.
Oponenti:

Datum obhajoby:

KLÍČOVÁ SLOVA

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

KEY WORDS

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

Dizertační práce je k dispozici na Vědeckém oddělení děkanátu FEKT VUT v Brně, Technická 10, Brno, 616 00

ISBN 80-214-
ISSN 1213-4198

Obsah

1 Sítě nové generace v České republice

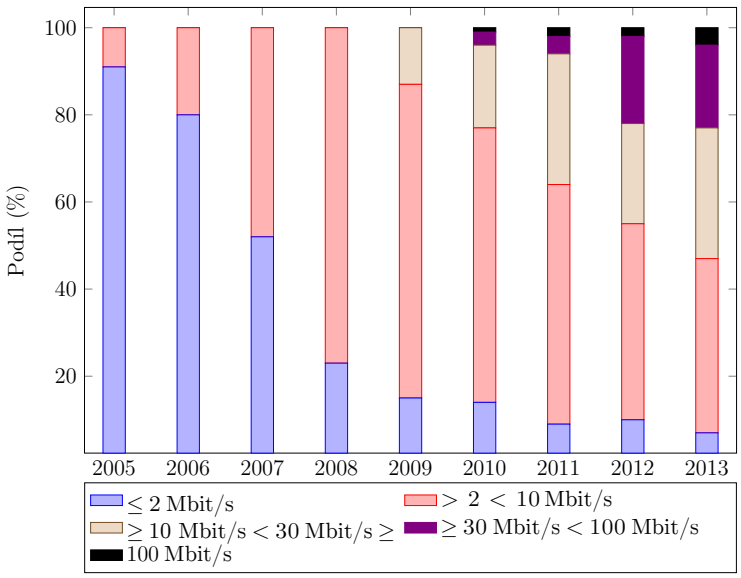
Česká republika se v rámci Evropské unie zavázala, že zajistí přenosovou rychlost alespoň 30 Mbit/s ve směru k uživateli do roku 2018 [1], dalším milníkem pak bude rok 2020, kde rychlost v sestupném směru má dosáhnout 100 Mbit/s pro polovinu domácností [1]. Obě uvedené varianty počítají s nesymetrickými přenosovými rychlostmi, tedy zpravidla vyšší rychlostí pro sestupný směr. Tento „nedostatek“ by měl být eliminován do roku 2030, neboť v tomto roce, na základě [2], je uvažována pouze symetrická varianta přístupu k Internetu.

Takovéto nároky na přenosovou rychlost již nedokáží splnit veškeré technologie např. ADSL (Asymmetric Digital Subscriber Line). V plánech České republiky se hojně zmiňuje pasivní optická síť typu GPON (Gigabit Passive Optical Network), nebo varianty aktivní optické sítě. Formální definici pro sítě nové generace lze na základě [3] definovat takto: NGN (Next Generation Network) 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.

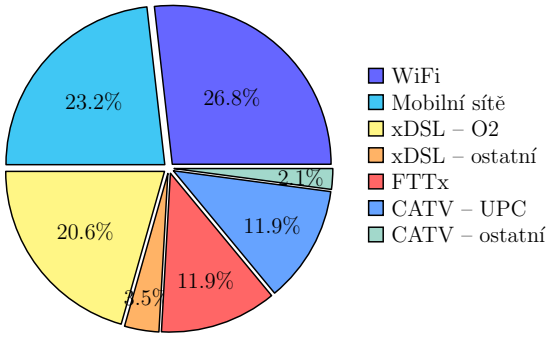
Na druhou stranu Česká republika není zcela připravena uspokojit vysoké nároky na rychlost připojení ve všech lokalitách. Na základě [4] vyplývá, že dominující přenosové rychlosti byly do 10 Mbit/s (viz obr. 1). Vyšší přenosové rychlosti nezaznamenávají významný růst.

V roce 2016 publikoval Český telekomunikační úřad výroční zprávu, kde je souhrn aktuálních technologií pro přístup k Internetu. Na základě obr. 2 je patrné, že dominující technologií je WiFi (26,8 %), tedy bezdrátový přenos informací. 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. Přípojky FTTx (Fibre to the ...) jsou na shodné hodnotě penetrace (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 (Fibre to the Home) variantě přenosovou rychlost až 10/10 Gbit/s[1] (sdíleně v závislosti na počtu koncových jednotek připojených k řídicí jednotce OLT).

[1] Při úvaze standardu dle [5].



Obr. 1: Vývoj přenosových rychlostí podle [4]



Obr. 2: Technologie pro přístup k Internetu v ČR na základě [6]

Obecně se rozlišují nejznámější FTTx přípojky:

- FTTN (Fiber to the Node) – 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 je přivedeno do účastnického rozvaděče (zpravidla na velkém sídlišti), od kterého vedou metalické rozvody ke koncovým zákazníkům.
- FTTB (Fiber to the Building) – 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 rozveden pomocí metalických spojů. V praxi se vyskytují i varianty, kdy jsou budovy propojeny vzájemně například bezdrátovým vysokorychlostním spojem.

- FTTH (Fiber to the Home) – 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 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) – v poslední době velice oblíbený styl zakončení optického vlákna ve vysílači rádiového signálu pokrývající danou oblast mobilním signálem.

Vlastnosti přístupových sítí nové generace podle [7] 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),
- poskytování podstatně vyšší přenosové rychlosti v sestupném směru, tedy ve směru k uživateli.

V současnosti se za odpovídající přístupové sítě nové generace považují [7]:

- 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 [7].

2 Cíle dizertační práce

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.

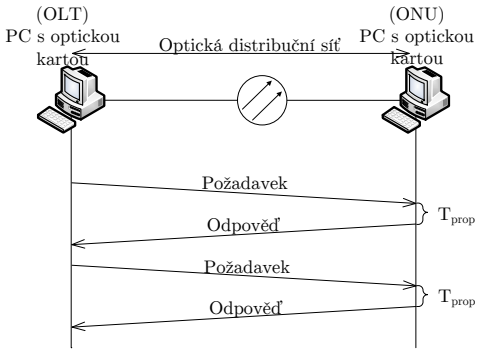
3 Hlavní výsledky práce

3.1 Návrh dodatečného parametru pro výměnu klíče

Zásadním nedostatkem dnešních GPON sítí 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). Charakter pasivní optické sítě spoléhá na připojení koncových zákazníků pomocí pasivního splitteru. 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) čas přenosu dat mezi OLT (Optical Line Termination) a ONU (Optical Network Unit). 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.

3.1.1 Experimentální ověření parametru T_{prop}

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). 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 (GPON Transmission Convergence) rámců [8]. Alternativní schéma k GPON síti je zobrazeno na obr. 3.



Obr. 3: 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[3]) s SFP (Small Form-factor Pluggable) 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.

Pro měření bylo využito protokolu ARP (Address Resolution Protocol) 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 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).

Tab. 1: 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. 1 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 ODN (Optical Distribution Network) o délce 20 a 40 km jsou $\approx$158 μs a $\approx$317 μs. Rychlost šíření pro 1 km jednovidového optického vlákna je $\approx$8 μs (včetně doby šíření a doby zpracování).

Na základě této znalosti lze odvodit, že naměřená hodnota 278 μs obsahuje dobu zpracování signálu odpovídající $\approx$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 [9].

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

3.2 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.

Navržený model předpokládá následující části:

- OLT – je řízeno poskytovatelem služeb je umístěno v CO (Central Office) 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[4].

- splitter – je pasivní optické zařízení, které slouží k připojení koncových zákazníků. Zpravidla je stále považováno za součást distribuční sítě.

3.2.1 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 3.1.

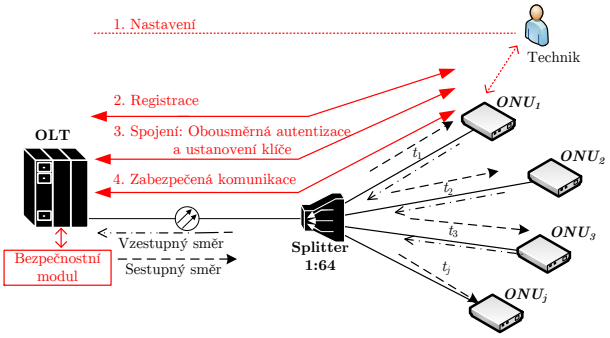
Navržený protokol pro ustanovení klíče je založen na ECDH (Elliptic Curve Diffie–Hellman) protokolu, jenž je modifikován na protokol SPEKE (Simple Password Exponential Key Exchange) [10]. Generátor *G* není vytvořen ve funkci jako u standardů IEEE P1363.2 a ISO/IEC 11770-4, ale bylo použito sdílené tajemství ve funkci HMAC (Keyed-Hash Message Authentication Code), 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] od/k zákazníkům z jejich domácí LAN (Local Area Network)

3.2.2 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.



Obr. 4: 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 [11]. 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 zobrazeno jako bezpečnostní modul). Tajný klíč technika $TSK\_n \in \{0,1\}^{256}$ je odvozován za použití KDF (Key Derivation Function), např. HMAC s SHA (Secure Hash Algorithm). 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

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.

Fáze spojení

Tato fáze poskytuje informace o ustanovení klíče a autentizaci. 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 $KU = H(M, HID\_i, t\_act)$, 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.

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 [12]. 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.

3.2.3 Experimentální implementace

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) a 512 MB RAM (Random Access Memory) s operačním systémem Linux Debian, které reprezentovalo ONU jednotku. OLT bylo zastoupeno PC (Personal Computer) 2,53 GHz CPU a 8 GB RAM s operačním systémem Windows 7. Výsledky měření zobrazuje tab. 2, která obsahuje čas běhu programu kryptografických operací na simulovaných zařízeních OLT a ONU během registrační a join fáze.

Tab. 2: 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

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. Celkově join fáze potřebuje 45,5 ms.

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 [13], [14] a [15].

3.3 Algoritmus pro detekci Rogue ONU

3.3.1 Komunikace v sestupném směru

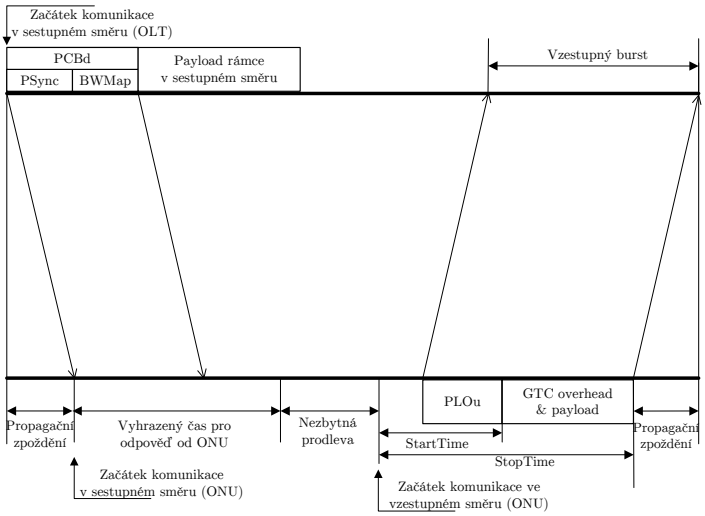
Sestupný směr je centralizován do OLT. OLT multiplexuje GEM rámce do přenosového média za použití GEM Port-ID. Identifikátor Port-ID odděluje koncové jednotky ONU, což znamená, že jeden rámec může obsahovat data pro více koncových ONU. Obecně si lze tyto identifikátory představit jako logické spojení 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.

3.3.2 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[5] [8]. 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 TCONT (Transmission Container) nebo OMCC (Optical Network Unit Management and Control Channel). 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. 5.

Nejdříve OLT připraví rámec s následujícími parametry: PCBd (Physical Control Block downstream), PSync, BWmap (Bandwidth Map) 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, 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. 5 je dále zobrazena hodnota, nezbytné zpoždění, která má za 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

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

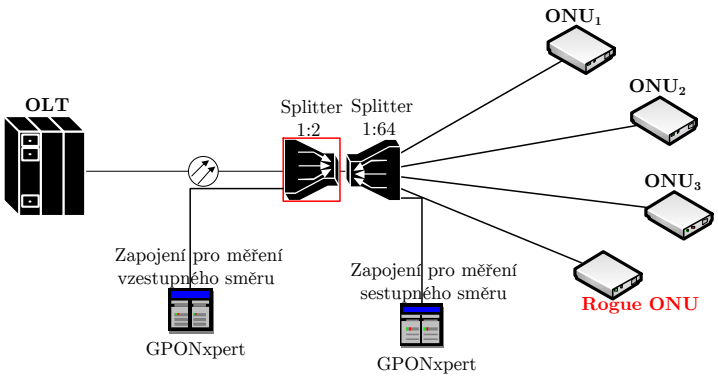


Obr. 5: Časová návaznost pro komunikaci ve vzestupné směru

specifikovaným OLT během Ranging stavu.

3.3.3 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[6]. Pro ukládání dat a jejich následné zpracování je použito FPGA polí. Níže uvedený obr. 6 zobrazuje zapojení pro měření obou směrů (postupné měření).



Obr. 6: GPON síť s modifikovaným (rougue) ONU

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

3.3.4 Výsledky měření

Scénář[7] byl zaměřený na měření připojené modifikované jednotky ONU (dále jen rogue ONU podle terminologie [8]). Nutno poznamenat, že rogue ONU se rozumí taková jednotka, která nerespektuje časové sloty.

Měření s připojenou rogue ONU prakticky „eliminuje“ veškerou funkční komunikaci na síti, díky nerespektování časových slotů. Ostatní jednotky opakovaně 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. 3) 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 [16] 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 [16].

Tab. 3 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).

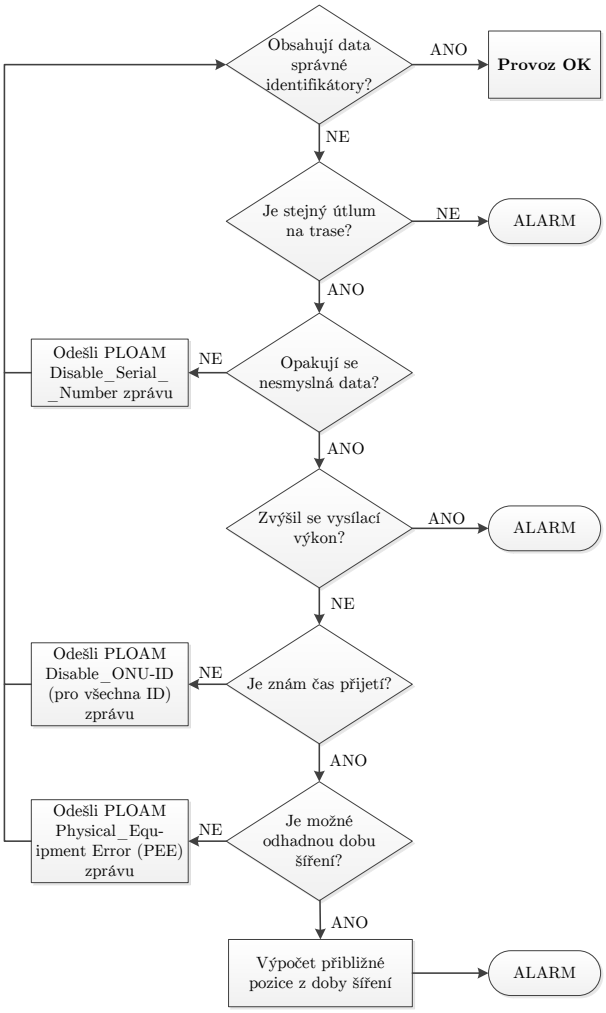
Tab. 3: Detaily provozu rogue ONU v reálné síti

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.	↑

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

3.3.5 Algoritmus pro detekci rogue ONU

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. 7.



Obr. 7: Nový algoritmus pro detekci rogue ONU

Navržený algoritmus startuje s ověřením unikátních identifikátorů, které má k dispozici každá ONU jednotka v distribuční síti (ONU-ID, Alloc-ID, T-CONT 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. 3 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 [17].

3.4 ILP model Triple Play

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. 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 1, 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 (Integer Linear Programming) model pokrývá dosavadní možnosti GPON sítí. Účelová funkce je následně definována jako:

$$max \sum_{i \in I, j \in J} W_j \cdot V_{ij} + \sum_{i \in I} k_i \tag{1}$$

S podmínkami:

$$\sum_{i \in I, \quad j \in J} W_j \cdot V_{ij} \leq C \tag{2}$$

$$V_{ij} = k_i \tag{3}$$

Pro účelovou funkci je nutné hlídat, aby nedošlo k překročení dostupné kapacity linky podle rovnice 2 a také přiřazování použitých služeb konkrétní ONU jednotce, jenž je nadefinovaná jako proměnná podle rovnice 3.

3.4.1 Dosažené výsledky vlastního ILP modelu

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.

```
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
;
C = 0
```

Z výpisu je zřejmé[8], 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.

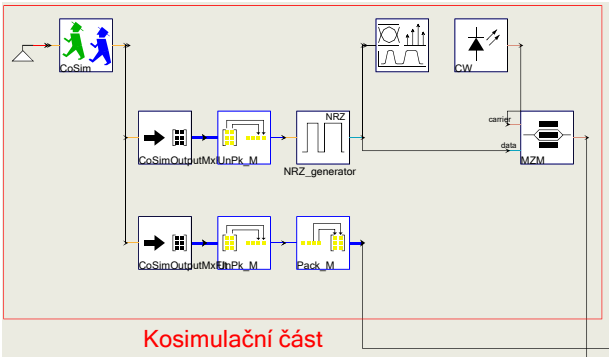
3.5 Implementace přenosové vrstvy NG-PON2

Neustálý nárůst požadavků na přenosovou rychlost a s tím související zvyšující se množství přenášených dat, které meziročně roste o 20–30 % [18], vede ke značnému navýšení přenosových rychlostí i v oblasti přístupových sítí. Posledním standardem pro PON sítě z dílny ITU (International Telecommunication Union) je standard NG-PON2 (Next Generation PON Stage 2).

3.5.1 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 (Time Wavelength Division Multiplexing 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. 8 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. 8: Navržená vysílací část pro NG-PON2

Distribuční část je tvořena vláknem typu G.657, které je navrženo pro přístupové

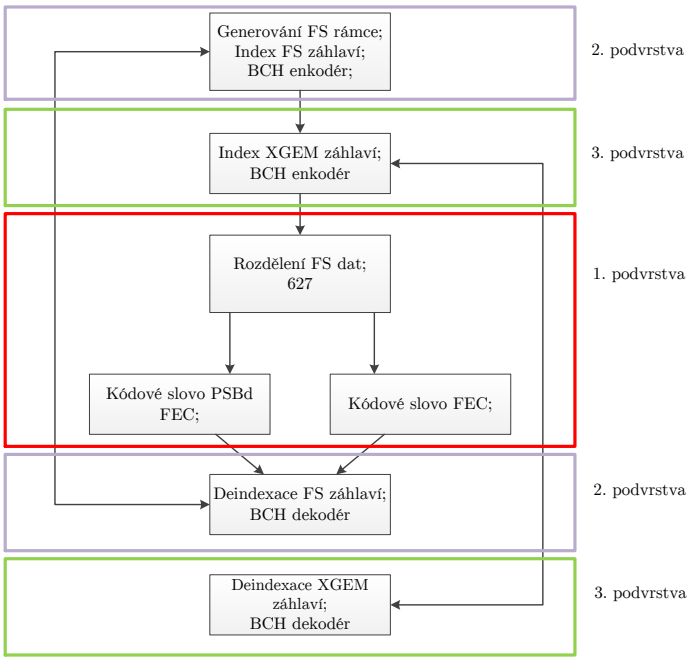
[8] Výpis je zkrácen.

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. Druhá implementace se opírá o spolupráci VPIphotonics s prostředím Matlab. 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. V reálné síti jsou koncové jednotky přeladitelné, pro zjednodušení simulace tato část není implementována.

3.5.2 Detekce chyb pro NG-PON2 sítě

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. 9.



Obr. 9: Model podvrstev v prostředí Matlab

Jelikož velikost XGEM (XG-PON Encapsulation Method) 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 (Hybrid Error Correction), což je kombinace BCH (Bose-Chaudhury-Hocquengham) 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[9]. Výsledkem je blok o velikosti 1728 bitů a po průchodu FEC 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 $\frac{1}{1083456} = 9,229 \cdot 10^{-7}$.

3.5.3 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 spolu s doporučenými výkonovými úrovněmi a citlivostí detektorů pro přenosovou rychlost 10 Gbit/s v sestupném směru.

Tab. 4: Útlumové třídy a jejich doporučené parametry

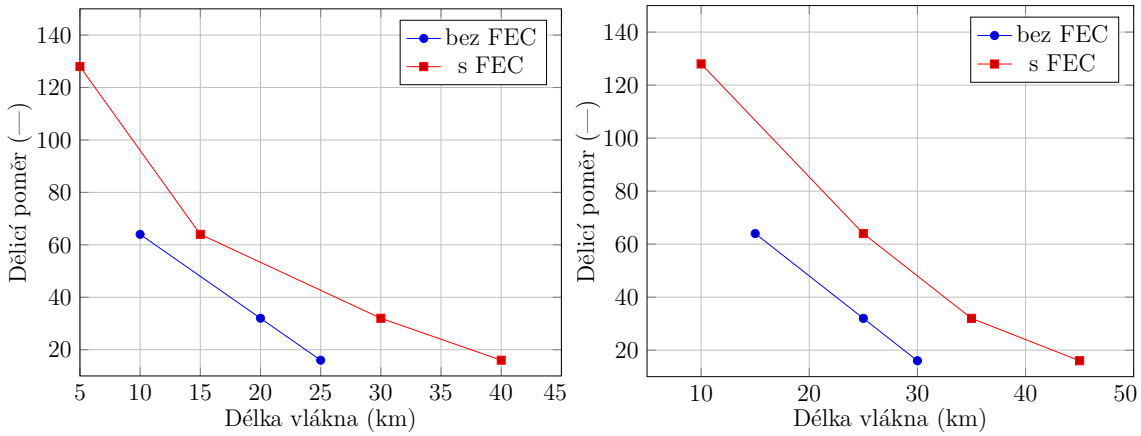
Útlumová třída	N1	N2	E1	E2
Minimální útlum [dB]	14	16	18	20
Maximální útlum [dB]	29	31	33	35
Min. výkon [dBm]	+3,0	+5,0	+7,0	+9,0
Max. výkon [dBm]	+7,0	+9,0	+11,0	+11,0
Minimální citlivost [dBm]	−28	−28	−28	−28
Maximální citlivost [dBm]	−7	−7	−7	−9

3.5.4 Výsledky simulací

Veškeré simulace byly rozděleny zpočátku podle útlumových tříd definovaných v [19]. Podle teoretických předpokladů pro útlumové třídy ODN v tab. 4 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 [19] uvádí i podporu dělicího poměru 1:256, nebyl tento poměr dělení brán v úvahu pro všechny simulace. Později v této podkapitole bude simulacemi dokázáno, že nejdelšího dosahu

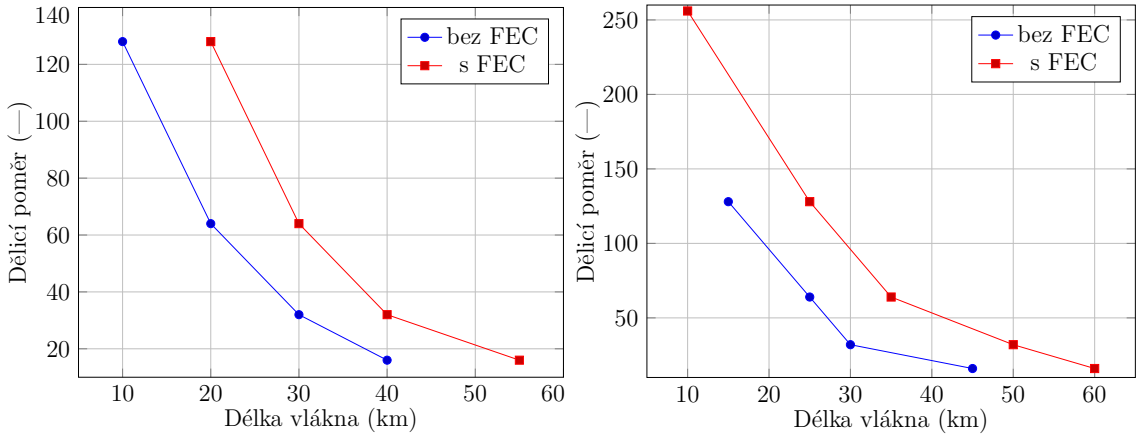
[9] Synchronizační struktury slouží k udržení synchronizace v sestupném směru pro všechny koncové jednotky. Vzorek dat je stále stejný.

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 (Bit Error Rate). 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.



Obr. 10: 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 (viz obr. 10) 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. 11: 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. 11. 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 [20].

4 Závěr

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 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. Jeden z cílů dizertační práce si klade za cíl zvýšení bezpečnosti za pomocí parametru T_{prop}. 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+. 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 para-

metru. 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.

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 přináší matematický model xPON sítí přenášející Triple Play služby (data, video a hlas). Model 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.

Poslední podkapitola je zaměřena na implementaci přenosové vrstvy do komerčně dostupného simulačního nástroje VPIphotonics. 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.

Literatura

[1] *Digitální Česko v. 2.0: Cesta k digitální ekonomice* [online]. Česká republika: Úřad vlády České republiky, 2012 [cit. 2016-10-07].

[2] *Poskytnutí informace - dokumentu Národní plán rozvoje sítí nové generace: (Strategie skokové změny 2030)* [online]. Česká republika: Ministerstvo vnitra České republiky, 2015 [cit. 2016-10-07].

[3] *Y.2001 : General overview of NGN* [online]. Švýcarsko: International Telecommunication Union, 2004 [cit. 2016-10-07].

[4] *Výroční zpráva Českého telekomunikačního úřadu za rok 2014* [online]. Česká republika: Český telekomunikační úřad, 2015 [cit. 2016-10-07].

[5] *G.987.2 : 10-Gigabit-capable passive optical networks (XG-PON): Physical media dependent (PMD) layer specification* [online]. Švýcarsko: International Telecommunication Union, 2016 [cit. 2016-08-14].

[6] *Výroční zpráva Českého telekomunikačního úřadu za rok 2015* [online]. Česká republika: Český telekomunikační úřad, 2016 [cit. 2016-10-07].

[7] *Národní plán rozvoje sítí nové generace: (pracovní verze ze dne – 5. srpna 2016)* [online]. Česká republika: Ministerstvo průmyslu a obchodu, 2016 [cit. 2016-10-07].

[8] *G.984.3 : Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification* [online]. Švýcarsko: International Telecommunication Union, 2014 [cit. 2016-07-14].

[9] 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.

[10] 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.

[11] 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.

[12] 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: Else-

vier GmbH, 2014, 125(3), s. 1361–1365. DOI: 10.1016/j.ijleo.2013.08.030. ISSN 00304026.

[13] 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.

[14] 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.

[15] 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.

[16] *G.Sup49 : Rogue optical network unit (ONU) considerations* [online]. Švýcarsko: International Telecommunication Union, 2011 [cit. 2016-07-16].

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

[18] Cisco. *The Zettabyte Era—Trends and Analysis* [online]. San Jose, USA: Cisco, 2016 [cit. 2016-08-17].

[19] *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].

[20] 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.

Stěžejní publikace 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.

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.

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.

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.

Curriculum Vitæ

Osobní údaje

Jméno:	Ing. Tomáš Horváth
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 disertační 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

- The 9th International Multi-Conference on Engineering and Technological Innovation (IMETI 2016).
- IJATES – Internet All-Electronic Journal, ISSN 1805-5443.
- Optica Applicata, ISSN 0078-5466.
- 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
H-index podle databáze WoS: 2

Poslední aktualizace dne **15. 5. 2017**

Abstrakt

Tato práce se zabývá optimalizací služeb Triple Play a bezpečností v optických přístupových sítích. První 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 podkapitola se věnuje analýze řídicího 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.

Abstract

This thesis deals with an optimization of Triple play services and security in optical access networks. The first 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 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.