VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Vladimír Spurný

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

ÚNIK INFORMACÍ PROSTŘEDNICTVÍM AKTIVNÍCH A PASIVNÍCH PRVKŮ V OPTICKÝCH VLÁKNOVÝCH INFRASTRUKTURÁCH

LEAKAGE OF INFORMATION THROUGH ACTIVE AND PASSIVE ELEMENTS IN OPTICAL FIBRE INFRASTRUCTURES

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — **Vladimír Spurný**

AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Petr Münster, Ph.D.**

SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Vladimír Spurný ***ID:*** 211810
Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Únik informací prostřednictvím aktivních a pasivních prvků v optických vláknových infrastrukturách

POKYNY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je teoretický rozbor problematiky úniku informací z optického přenosového systému. Analyzovány budou nejen metody úniku informací z optického vlákna, ale i z aktivních a pasivních prvků v přenosové soustavě. V rámci praktické části práce bude proveden návrh a ověření vybraných metod na vytvořeném testovacím pracovišti. U všech metod bude provedena analýza rizik včetně návrhu možností minimalizace/eliminace rizik.

DOPORUČENÁ LITERATURA:

[1] KEISER, Gerd. Optical fiber communications. 4th ed. New York, NY: McGraw-Hill Companies, c2011. ISBN 0073380717.

[2] JUNG KARKI, Sachin. Hacking Fiber optics easier than copper cable: Freelance IT Security professional [online]. 2016 [cit. 2019-09-14]. Dostupné z: http://bit.ly/2lOHXS8

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: doc. Ing. Petr Münster, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Tato bakalářská prace se zabývá problémem úniku informací z optických vláknových infrastruktur, a to jak ze samotných vláken, tak z pasivních i aktivních prvků. První část je věnována teoretickému popisu přenosu informací po optickém vláknu a funkci jednotlivých komponent. Další část je zaměřena na teoretický rozbor možných úniků informací. V poslední – praktické části dojde k prověření některých již předem popsaných možností úniku informací s následnou analýzou a návrhem minimalizace rizik.

KLÍČOVÁ SLOVA

únik informací, bezpečnost, vláknové infrastruktury, přenosový systém, optické vlákno, GPON, riziko, odposlech

ABSTRACT

This bachelor thesis deals with the problem of information leakage from optical fiber infrastructures, both from the fibers themselves and from passive and active elements. The first part is devoted to a theoretical description of the transmission of information over an optical fiber and the function of individual components. The next part is focused on the theoretical analysis of possible information leaks. In the last - practical part, there will be an examination of some of the previously described possibilities of information leakage with subsequent analysis and a proposal for risk minimization.

KEYWORDS

information leakage, security, fiber infrastructure, transmission system, optical fiber, GPON, risk, eavesdropping

SPURNÝ, Vladimír. *Únik informací na aktivních a pasivních prvcích optických vláknových infrastruktur*. Brno, 2030, 65 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: doc. Ing. Petr Münster, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Únik informací na aktivních a pasivních prvcích optických vláknových infrastruktur“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících 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

PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval vedoucímu své bakalářské práce panu doc. Ing. Petru Münsterovi, Ph.D. za příkladné vedení, ochotu, dávku trpělivosti a smysluplné konzultace, které mi v průběhu zpracování bakalářské práce věnoval.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Už od pradávna žene člověka v rozvoji dál chuť objevovat svět, navzájem komunikovat a vzdělávat se. Za poslední století došlo k extrémnímu urychlení vývoje v oblasti přenosu informací jak lokálně, tak globálně. S narůstajícím chtíčem po množství informací, které každý člověk a systém denně potřebují zpracovávat, jsme byli nuceni objevit nové způsoby přenosu informací.

V 60. letech 20. století společně s vynálezem laseru dochází k prvnímu rozvoji na poli optických přenosových soustav. Vlivem nedostatku technologií nebylo možné vyrábět optická vlákna bez kazů, skleněné vlákno nebylo dostatečně kvalitní. Až v roce 1970 se daří vědcům vytvořit něco provozuschopného, co má více výhod než nevýhod. V průběhu dalších let dochází k neustálému zdokonalování technologie. Okolo roku 1978 jsou instalovány optické kabely celosvětově a ustálila se vlnová délka na které tyto systémy pracují. Jedná se o vlnové délky od 770nm do 1675nm. V 90. letech vzrůstá poptávka po potřebě velké šířky pásma, to vlivem rozmachu domácích pracovních stanic a jejich neustálým vývojem, bylo tedy nutné přijít s lepším řešením. Šlo o vlnový multiplex, díky kterému se začalo do jednoho vlákna vysílat na více vlnových délkách. Díky tomu se z optických vláken stal neporazitelný hráč v oblasti přenosu velkého množství dat. Vývoj této technologie pokračuje až do dnešních dní, optický kabel už není jen ojedinělou záležitostí, ale něčím, s čím se pravidelně setkává velké množství populace, ač o tom nemusí ani vědět. [1]

Každá věc má ale i své stinné stránky, ač se zdá, že optické vlákno je přenosové médium, jež je nemožné odposlouchávat, opak je pravdou. Už v 90. letech se objevují první náznaky. Al-Quada odposlouchávala konverzace mezi USA a jejími ambasádami, Severní Korea byla přichycena při provádění špionáže. Na začátku nového tisíciletí došlo k odposlechu hlavních linek Deutsche Telecom a skrz optickou síť firmy Verizon uniklo obrovské množství citlivých dat. Odposlech na optických přenosových soustavách je tedy problémem jak rozlehlých sítí (WAN), tak i menších metropolitních sítí (MAN), anebo sítí malých poskytovatelů připojení. [1]

Tato práce se zabývá analýzou nejběžnějších možností úniků dat jak na pasivních, tak i aktivních prvcích optického přenosového systému. V praktické části se hlavně zaměřuje na únik informací za pomocí vložení optického děliče, únik informací způsobený absencí absolutního odrazu vlivem makroohybů, spektrální analýzu přeslechů u různých typů multiplexorů a v neposlední řadě se věnuje bezpečnosti standardu GPON.

1 Přenos informace na optických vláknech

Přenos informace umožňuje záření, které díky totálnímu odrazu prostupuje až na konec optického vlákna, nosičem informací jsou tedy fotony. Na rozdíl od elektronů v případě metalických kabelů. Optický spoj se skládá ze 3 základních komponent. Z vysílací části, přenosového prostředí a přijímací části. Vysílací část je tvořena zdrojem záření – laserem nebo luminiscenční diodou, které se následně moduluje. V přijímací části je fotodetektor, který převádí signál zpět na elektrický. Poslední částí je samotné přenosové prostředí, které se skládá z optických vláken a dalších aktivních nebo pasivních prvků, jako jsou děliče nebo zesilovače. Užití těchto prvků nám dovoluje propojovat stále větší vzdálenosti a přenášet stále větší objemy dat. [2]

1.1 Šířka pásma

Šířka pásma udává nejvyšší frekvenci, kterou může být přenášen signál na vzdálenost 1 kilometru, aniž by došlo k poklesu amplitudy signálu na 1/2, tedy o 3 dB. Velikost šířky pásma je udávána v MHz.km. Pro každou vlnovou délku je šířka pásma jiná. U vlákna s šířkou pásma 160 MHz.km při vlnové délce 850 nm. Pro stejné vlákno je šířka pásma u vlnové délky 1310 nm rovna 500 MHz.km. [3]

1.2 Numerická apertura

Numerická apertura popisuje největší možný úhel světelného paprsku vzhledem k ose optického vlákna, pod kterým může optický paprsek vstupovat do optického vlákna, aby došlo k absolutnímu odrazu mezi jádrem a pláštěm vlákna. Pokud paprsek vstoupí do vlákna pod větším úhlem, než je NA, nedojde k absolutnímu odrazu, ale k lomu a paprsek zaniká v plášti vlákna. [3]

Vztah pro výpočet NA:

$$\mathrm{NA} = \sin_a = (n_1^2 - n_2^2)$$

a je mezní úhel navázání, kdy n_1 je index lomu jádra a n_2 plášť. Z toho vyplývá, že vláknem se budou šířit všechny paprsky vstupující do vlákna pod úhlem menším neboj stejným, než je úhel mezního navázání. [3]

1.3 Chromatická disperze

Chromatickou disperzi zapříčiňuje fakt, že vstupní paprsek nikdy není monochromatický, skládá se ze složek s různými vlnovými délkami a každá složka se šíří vláknem jinou rychlostí. Na konec vlákna každá složka dorazí v rozdílném čase. Vlivem zpoždění určitých složek dochází k časovému roztažení přenášených impulzů a zkreslení přenášené informace. Pro jednovidová vlákna je chromatická disperze nejmenší při přenosu na vlnové délce 1310 nm. Chromatická disperze je tvořena dvěma složkami - materiálovou a vlnovodnou disperzí. [4]

Materiálová disperze

Materiálová disperze je závislá na indexu lomu použitého materiálu jádra optického vlákna, většinou se jedná o sklo, kdy typická hodnota indexu lomu jádra je okolo 1.48. Dále závisí na vlnové délce, přičemž každá vlnová délka se šíří materiálem jinou rychlostí, z toho vyplývá, že rychlost šíření signálu narůstá s vlnovou délkou a je jí tedy přímo úměrná. [3]

Vlnovodná disperze

Vlonovodnou disperzi způsobují geometrické vlastnosti vlnovodu, jako je například nehomogennost materiálu jádra, jež vytváří prostředí s lehce jiným indexem lomu. Při změně vlnové délky dochází ke změně tvaru podélného vidu. Vlnovodná disperze zpomaluje vlnu nepřímo úměrně vlnové délce, díky tomu můžeme vzájemně disperze vykompenzovat. [3]

1.4 Polarizační disperze

Při užití singlemode vláken se vid šíří ve dvou vzájemně kolmých polarizačních rovinách. Vlivem nehomogennosti a nedokonalosti vlákna, která prochází buď z výroby, kdy vlákno nemá v určitých částech dokonale kruhový průřez či mikroohyby, nebo jiným narušením při tažení optického vlákna dochází k vzájemnému opoždění/posunutí daných vidů. Tuto disperzi nedokážeme nijak kompenzovat, protože při jakékoli změně trasy, např. natažením jiné kabeláže stejnou trasou dojde k dalším ohybům nebo tlakům na vlákno a tedy i ke změně vidové disperze. Oproti předchozím druhům disperze je polarizační desperze při malých přenosových rychlostech téměř zanedbatelná, avšak při rychlostech přesahujících 2.5 Gb/s se stává důležitým parametrem. [3]

1.5 Měrný útlum

U optických vláken, podobně jako u vláken metalických dochází k postupnému poklesu výkonu signálu s rostoucí vzdálenosti od zdroje záření. Útlum udáváme v decibelech – dB. Jedná se o poměr vstupního (P_1) a výstupního výkonu (P_2). Vyjadřuje celkové množství ztrát signálu na trase. Největšími působiči útlumu jsou absorpce a rozptyl. Celkový útlum je roven součtu všech podsložek. [5]

Vztah pro výpočet útlumu:

$$\text{u()}=10^{*}\log(P_1/P_2)[\text{dB}]$$

1.5.1 Absorbce

Největším působitelem útlumu na optických vláknech je absorpce, dělíme ji na vlastní a nevlastní. Vlastní absorpci způsobují molekuly jádra, nejčastěji SiO_2, které část záření pohltí, tento materiál dosahuje absorpčního maxima jak v UV tak IR oblasti. Nevlastní absorpci způsobují přechody mezi základními materiály a nečistotami – ionty OH, jejichž druhá a třetí harmonická rezonančního kmitočtu spadá do oblasti využívaného pásma, a také ionty kovů, zejména Fe, Cu a Cr, které se do jádra dostávají při výrobě. Malý obsah těchto iontů je základním faktorem vlákna s malým útlumem, typicky pod 1 dB/km. V dnešní době jsou vyráběna vlákna s označením LWP (low water peak), která mají velmi malý obsah iontů vody. [5]

1.5.2 Rozptyl

Vlákna jsou nejčastěji vyráběna z SiO_2. Jedná se o amorfní látku, která nemá krystalovou mřížku. Při chladnutí materiálu dochází ke vzniku nehomogenit. Tyto nehomogenity jsou způsobeny náhodným ukládáním molekul SiO_2 a dalších látek. Díky tomu vznikají části s lehce rozdílnými indexy lomu, na nichž je paprsek rozptýlen všemi směry a dochází k útlumu signálu. Mezi materiálové rozptyly řadíme Reyleigův rozptyl, Mieův rozptyl nebo rozptyl způsobený nečistotami. [5]

Rayleighův rozptyl

Jedná se o jev vznikající tepelnými kmity molekul v nepravidelné mřížce. Vlivem tepelných kmitů, mikrozměn ve vlákně, dochází k rozptylu části záření. Tohoto jevu se nedokážeme zbavit ani při ochlazení vlákna na absolutní nulu, kdy dojde k pozastavení veškerého pohybu na molekulární úrovni. I za takové situace se světelný paprsek ohýbá okolo jader atomů v molekulách. [5]

Mieův rozptyl

Způsoben nedokonalostmi, které mají srovnatelnou velikost jako vlnová délka záření. Příčinami mohou být mikroskopické bublinky, nedokonale kulaté vlákno atd.. Pokud velikost takových nedokonalostí přesáhne 1/10 vlnové délky dochází k razantnímu zvětšení rozptylu. Možností, jak eliminovat tento rozptyl je zvýšení kvality výroby. [5]

Rozptyl vlivem přítomnosti nečistot a špatného výrobního postupu

Může se jednat o rozptyl způsobený množstvím nečistot v materiálu jádra, trhlinkami vzniklými špatným tažením vlákna nebo nepravidelnými změnami průměru jádra či pláště. Všechny tyto možnosti jsou způsobeny špatnými výrobními procesy. Tyto chyby jsou makroskopické velikosti. [5]

1.6 Nelineární jevy

Nelineární materiálový rozptyl

Pokud dochází ve vláknu k materiálovému rozptylu, mají v drtivé většině případů rozptýlené fotony stejnou frekvenci jako fotony, které nebyly rozptýleny, občasně ale může dojít k tomu, že foton je rozptýlen s jinou frekvencí. Tento jev způsobuje neúměrnost vstupního a výstupního výkonu. [6]

Brillouiniův rozptyl

Tento rozptyl zapříčiňuje akustická vlna působící změnu indexu lomu, kvůli které dojde k vytvoření akustického fotonu, který zapříčiní zpětný frekvenční posuv. Pro minimalizaci tohoto rozptylu je vhodné použít širší spektrum přenosu.[6]

Ramanův rozptyl

Působením prostředí na přenášený signál může dojít k frekvenčnímu posunu, tento jev může mít i pozitivní důsledky – viz kap 2.7 – Ramanovský zesilovač.

Generování druhé harmonické

K tomuto objevu došlo po vynálezu rubínového laseru, jímž byl prosvěcován křemenný krystal. Výstupní frekvence byla přesně dvojnásobná. U optických vláken lze tento jev pozorovat, pokud jsou dotována fosforem nebo germaniem. Pro klasická optická vlákna je vzhledem k jejich středové symetrii možné s velmi malou účinností generovat až 3. harmonickou. [6]

Třívlnný proces

Při průchodu dvou harmonických vln nelineárním prostředím dochází ke vzniku třetí vlny, jejíž frekvence je rovna součtu nebo rozdílu dvou vstupních vln. [6]

Čtyřvlnné směšování

Vzniká při navázání 3 paprsků v nelineárním prostředí, jako u třívlnného procesu, ale s různou vlnovou délkou, a projeví se vznikem čtvrté rozdílné vlny. Jedná se o závažný problém při realizaci DWDM přenosů. [6]

1.7 Spektrum přenosu

Jak již bylo zmíněno v úvodu, tak se spektrum vlnových délek ustálilo v oblasti od 770 nm do 1675 nm, toto spektrum se následně dělí na menší pásma. [7][1]

Název pásma	Vlnová délka [nm]	Způsob užití
850 nm - band	770 - 910	Primárně pro multimode systémy
O-band (original)	1260 - 1360	Historicky první pásmo, používáno v 70. letech, nejmenší útlum pro tehdy produkovaná vlákna
E-band (extended)	1360 - 1460	Nejméně používané, měly nejvyšší útlum kvůli OH iontům
S-band (short-wawelenght)	1460 - 1530	Primárně pro downstream u pasivních optických sítí
C-band (conventional)	1530 - 1565	Často užíváno pro spoje na dlouhé vzdálenosti
L-band (long-wavelenght)	1565 - 1625	Použito v systémech užívajících vlnový multiplex
U-band (ultra-long-wavelenght)	1625 - 1675	Primárně určeno pro monitoring sítě

Tab. 1.1: Pásma vlnových délek

2 Optické sítě

2.1 Zdroje záření

Hlavním úkolem zdroje optického záření je převedení elektrických signálů na formu, kterou jsou schopna přenášet optická vlákna. Nejčastěji se jedná o LED a laserové diody. [8]

LED

LED je elektroluminiscenční dioda. Vyzařuje záření díky průchodu elektrického proudu P-N přechodem v propustném směru. Díky malé intenzitě vyřazování s nízkou spínací frekvencí jsou používány v multimode systémech s malou přenosovou rychostí. [8]

Laserová dioda

Laserová dioda dunguje na principu stimulované emise záření, které vlastnostmi odpovídá laserovému záření – je monochromatické. Emituje záření s velmi silnou intenzitou a je proto využívána v singlemode systémech, ve kterých je zapotřebí vysoká rychlost přenosu. [8]

2.2 Druhy optických vláken

2.2.1 Vícevidová vlákna

Nejčastěji jsou používána pro komunikaci na krátké vzdálenosti. Vlákno má tlustší jádro, typicky 50 nebo 62.5 mikrometrů, vlivem toho dochází k šíření mnoha paprsků (vidů) vláknem. Vlákno má velkou kapacitu, spolehlivost a je levnější než jednovidové vlákno. Používá se jako páteřní rozvod pro LAN sítě. Díky větší velikosti jádra můžeme používat levnější zdroje záření, například LED. Vícevidová vlákna se dále dělí na vlákna se skokovým indexem lomu, kdy plášť i jádro mají daný index lomu. Paprsky se v něm šíří totálními odrazy, dochází zde k vidové disperzi, která omezuje délku přenosu na krátké vzdálenosti. Dalším druhem jsou vlákna s gradientním indexem lomu. S narůstající vzdáleností paprsku od osy jádra je index lomu menší. Paprsek opisuje sinusovou křivku a nedochází k vlnové disperzi, a tedy k menšímu zkreslení. Tento druh kabelu má oranžovou barvu pláště. [9]

2.2.2 Jednovidová vlákna

Jedná se o druh optického vlákna s tenkým jádrem, na kterém se přenáší pouze jeden vid, jeden paprsek. Tyto vlákna mají velmi malé jádro (typicky okolo 10 mikrometrů), které dráhu záření napřimuje a nedochází k jeho rozptylu. Díky tomu dokáží jednovidová vlákna vést paprsky na dlouhé vzdálenosti. Typicky jsou užívána jako přenosové médium v páteřních sítích. Vzhledem k velikosti jádra je třeba použít přesnější generátor i detektor záření. Jednovidová vlákna mají žlutou barvu vnější ochrany a jejich cena je typicky vyšší než u vícevidových vláken. [9]

2.3 ITU standardy

Jsou to standardy mezinárodní telekomunikační unie. ITU je reprezentována téměř dvěma sty státy. ITU spravuje mimo jiné i běžně odkazované dokumenty ohledně single-mode optických vláken, tak jak to požadují výrobci telekomunikačních systémů. Konkrétně jde o standardy G.652 až G.655 a G657. [10]

G.652

Jedná se o NDSF typ optického vlákna standardizovaného v roce 1984. Dále se dělí na další 4 typy označovány písmeny A, B, C, D. Vlákno vyrobené dle tohoto standardu je typické téměř nulovou disperzí pro vlnovou délku 1310 nm, vlivem zbytkových OH molekul není vhodné použití typů A a B v systémech užívajících vlnový multiplex. Varianty C a D tento problém řeší, díky tomu můžeme používat vlákna standardu G.652 téměř v celé oblasti přenosového spektra. Nevýhodou těchto vláken je špatná odolnost vůči ohybům, která je vyřazuje ze hry v exponovaných prostorech (byty a kanceláře). [10]

G.653,654

Tento standard označuje optická vlákna s minimální disperzí pro vlnovou délku 1550 nm.[10]

G.655

Standardy určující jednovidová vlákna, jež mají malou chromatickou disperzi v pásmu C, dělí se na 2 typy dle sklonu proti vlnové délce. Disperze dokáže potlačit čtyřvlné směšování a další nelineární efekty, které jsou velkým problémem při použití vlnového multiplexu, proto splňují požadavky DWDM přenosu. [10]

G.657

Označuje jednovidová vlákna s menší citlivostí na makroohyby. Slouží pro kratší aplikace, například v domácnostech, kde jsou využívány díky poměrně větší odolnosti oproti vláknům patřícím pod standard G652, nebo na místech náchylných k odposlechu pomocí fibre tappingu.[10]

2.4 Spojování optických vláken

Existují 2 způsoby spojování optických vláken. Mechanicky, kdy dojde k extrémně přesnému zarovnání vláken vůči sobě a následnému zafixování speciálním přípravkem. Vlákna nejsou permanentně spojena což umožňuje jejich rozpojení bez následného porušení. Mechanické spoje mají oproti svarům větší útlum, okolo 0.3 dB. [8]

Druhým způsobem je svařování. Konce vláken jsou vložena do optické svářečky, která je srovná a následně za použití elektrického oblouku roztaví a spojí. Spoj je poté opatřen ochranou sváru, aby nedošlo k jeho přelomení. Tyto přístroje dokáží zároveň opticky změřit útlum a prověřit pevnost optického sváru v tahu. Typický útlum optického sváru je okolo 0.1 dB, referenční hodnota je 0.2 dB. Svařování je tedy mnohem spolehlivější. Nejčastěji je používáno k zakončování optických tras za pomoci konektorů – pigtailů. [8]

2.5 Druhy optických konektorů

Optické konektory slouží k propojování prvků. Jsou používány tam, kde je potřeba mít možnost přepojovat prvky. Existuje mnoho typů, které se liší způsobem užití. Mezi nejznámější patří konektory SC, ST, FC a LC. Dalším rozlišovacím faktorem je typ broušení čela ferule. Ferule je část konektoru, která se stýká s druhým konektorem. Je to válec, typicky o průměru 2.5 mm, v jehož středu je zafixováno optické vlákno. Broušení ferule je prováděno z důvodu zvýšení útlumu zpětného odrazu (ORL – optical return loss), které je možno ve 4 variantách PC (ORL= -30 dB), SPC (ORL= -40 dB), UPC (ORL= -50 dB) a APC, kdy je čelo ferule zbroušeno v úhlu 8^{o}, díky tomu dosahujeme útlumu zpětného odrazu až -60 dB. APC konektory mají zelenou barvu a jsou dostupné pouze pro singlemode. S rostoucí kvalitou konektorů klesá měrný útlum, u kvalitních konektorů typicky pod 0.5 dB. [11]

SC

Jsou užívány jak pro single-mode, kde je možnost APC broušení, tak i pro multi-mode, a jsou vyráběny v simplex i duplex variantách. Jedná se o nejpoužívanější konektory díky jejich ceně a jednoduchosti. Jsou konstruovány na 1000 párovacích cyklů oproti většině konektorů, které jsou konstruovány na 500 párovacích cyklu. Po rozmachu Gbit prvků užívajících SFP byly částečně nahrazeny LC konektory. [12]

ST

Jedná se o dříve nejpoužívanější konektory pro multi-mode vyvinuté společností AT&T. Jsou bajonetové s dvojí možností připojení – push in a twist. Vzhledem ke konstrukci byl občasný problém se správným dosednutím. Dnes již málo používaný. [12]

FC

Tento konektor je stavbou podobný ST konektoru, ale se závitem a polohovatelným zářezem. Dříve byl velmi hojně používán pro single-mode. Nabízí extrémně přesné uložení. Dnes již téměř nepoužívaný. [12]

LC

Jedná se o SFF – small form factor konektor, který je nejpoužívanější u Gbit prvků, za jeho rozmach může společnost Cisco. Používán v SFP modulech. Oproti ostatním má poloviční keramickou feruli (1,25mm), která zajišťuje přesné vyrovnání. Jejich upevnění je zajištěno jazýčkem, díky kterému jsou řádně zafixovány, ale vzhledem ke kterému jsou dimenzovány na 500 párovacích cyklů. Typický útlum je 0,25 dB. Stejně jako SC konektory jsou vyráběny v simplex i duplex variantách. [12]

2.6 Optický dělič

Optický dělič (splitter) je důležitý pasivní prvek optických přenosových sítí. Jeho hlavní funkcí je pasivní rozdělování optických signálů bez jakýchkoliv dalších úprav na 2 nebo více v sestupném směru. Ve vzestupném směru probíhá slučování optických signálů na jeden. Existují 2 výrobní technologie – FBT a PLC. [11]

FTB dělič

Jedná se o nejběžnější optické děliče, fungující na principu spojených optických vláken. Ke spojení dochází za vysokých tlaků a teplot, kdy dojde k roztavení pláště a přiblížení jader vláken těsně k sobě. Vzniknou svazky 2 až 4 vláken, která se následně kaskádovitě skládají za sebe. Typicky jsou tyto děliče použity pro menší počty výstupních portů. [11]

PLC dělič

Je typ děliče fungujícího na polovodičové technologii. Dělič obsahuje jeden PLC čip a odpovídající počet optických polí. Tato struktura je vytvořena na křemíkovém substrátu. Tyto děliče mají poměrně menší útlum oproti FBT děličům a dokáží dělit až v poměru 1:128. Jsou tak velice vhodné do PON sítí. [11]

2.7 Optické zesilovače

Zesílení signálu

Pro přenos dat na extrémně dlouhé vzdálenosti bylo zapotřebí signál zesílit nebo obnovit. Nominální hodnota měrného útlumu u kvalitních vláken dosahuje 0.2 dB na km, proto u spojů délky okolo 10 km a více nemůžeme tento faktor přehlížet. Existují 2 možnosti zesílení signálu. Tou složitější je převod optického signálu na elektrický, následné zesílení a převedení opět na signál optický. Tento proces je náročný. Druhou možností je signál zesílit opticky. Optický zesilovač je tady nedílnou součástí komunikace na dlouhé vzdálenosti. [13]

EDFA zesilovač

Funguje na principu dopování optického vlákna ionty erbia. Hlavní výhodou je, že signál je posilován na více vlnových délkách, tyto zesilovače jsou proto vhodné pro použití v systémech užívajících WDM a jejich rozmach způsobil razantní nárůst zvýšení kapacity přenosových systémů. Nevýhodou je vznik chromatické disperze kvůli přítomnosti mnoha spektrálních složek. [13]

Ramanovský zesilovač

Užívají stimulovaný Ramanův rozptyl k zesílení signálu. Za pomoci budiče je možné posílit fotony rotační energií molekul prostředí. Dochází k přesunu energie z nižších vlnových délek (vlnová délka laseru zesilovače) směrem k vyšším vlnovým délkám (vlnová délka přenosu). Pro přenos na vlnové délce 1550 nm dochází největšímu zisku při posunu o cca 100 nm (13,2 THz), z čehož vyplývá, že pro potřebu zesílení signálu o této vlnové délce použijeme budič pracující na vlnové délce 1450 nm. [13]

2.8 Vlnový multiplex - WDM

Vlnový multiplex pracuje na principu vysílání na několika vlnových délkách jedním optickým vláknem. Přičemž největší výhodou této metody je, že se dá implementovat na již existující optické trasy. Nejjednodušším řešením je WDM na dvou vlnových délkách z různých „oken“, např. 1310 nm a 1550 nm pro jednovidová vlákna a 850 nm a 1300 nm pro mnohovidová vlákna, kdy můžeme provozovat plně duplexní spojení nebo zvýšit přenosovou kapacitu na dvojnásobek. Dalšími způsoby realizace WDM jsou WWDM, CWDM a DWDM. Jednotlivé multiplexy se liší velikostí odstupu jednotlivých kanálů, které u WWDM dosahovaly 25 nm, u CWDM 20 nm, kdy je používáno 18 kanálů od vlnové délky 1260 nm po vlnovou délku 1620 nm. U metody DWDM činí odstup kanálů 1,6 nm nebo 0,8 nm, přičemž laboratorně až 0,4 nm, což umožňuje přenášet terabity za sekundu. [3]

2.9 Multiplexer a demultiplexer

Tato zařízení slouží pro slučování a následné rozlučování vlnových délek do jednoho vlákna, jedná se tedy o nedílnou součást WDM spojení. Multiplexer může být realizován jako sdružovač s několika vstupy nebo jako multispektrální zdroj s přeladitelnou vlnovou délkou. U delmultiplexeru používáme difrakční mřížky, hranol nebo optický filtr. U malého počtu vlnových délek je vhodné užití optických filtrů. U většího počtu vlnových délek je třeba užít difrakci. Mezi nejběžnější demultiplexery patří soustavy dielektrických filtrů, AWG a FBG multiplexery. [15]

Soustava dielektrických filtrů

Slouží k postupnému odfiltrování dílčích optických signálů. V rámci soustavy filtrů je na každém z nich odfiltrována jedna frekvence na snímač a zbytek je propuštěn dále. Celý proces se opakuje dokud se neodfiltrují postupně všechny složky. [15]

AWG - arrayed waveguide grating

Tyto demultiplexery jsou používané v souvislosti s DWDM. Multiplexer se skládá ze dvou odbočnic, přičemž první z nich rozvětví signál na jednotlivé části, následně jsou tyto rozdělené signály vedeny paralelními dráhami s rozdílnou délkou, díky které dojde k fázovému posunu. Na druhé odbočnici dochází k rozdělení na výstupní větve vlivem interference. [15]

FBG - Fibre bragg grating

FBG pracuje na podobném principu jako dielektrické filtry, kdy k odrazu od mřížky dochází, pokud je vlnová délka vstupní vlny téměř rovna Braggově rezonanční vlnové délce, jinak signál prochází dále. Braggova mřížka je periodická struktura vytvořená UV laserem v jádru optického vlákna, kde vznikají oblasti s odlišnými indexy lomu. Mřížka splňuje Braggovu podmínku difrakce, která vyžaduje velikost periody změny indexu lomu rovnu polovině vlnové délky, změnou periody tedy regulujeme, jaká frekvence je odfiltrována. [15]

2.10 Optické přístupové sítě OAN

Vzhledem ke zvyšujícím se nárokům na metalická vedení došlo k prostupu optických tras i do nižších úrovní sítí. V dnešní době jsou stále více používána optická vlákna, která jsou instalována až do domácností – FTTH (fibre to the home). Z dlouhodobého hlediska je tento krok velmi výhodný, protože u optického vlákna dosáhneme jejich limitů mnohem později než u klasickéh metalické kabeláže, kdy do domácností jsou nejčastěji vedeny kabely kategorie 5E, které jsou normovány na přenos maximálně 1 Gbit/s. V těchto ohledech optika metalické rozvody mnohonásobně překonává. OAN dělíme na 2 základní druhy - sítě aktivní AON a pasivní PON.

AON - active optical network

Aktivní optická síť využívá aktivní prvky, její výhodou je organizovanější distribuce dat k uživatelům a možnost přenášet data na delší vzdálenosti, konkrétně až 70 km bez potřeby signál zesilovat. Ke každému uživateli putují pouze informace pro něj určené a žádné jiné, což zajišťuje určitou bezpečnost vůči odposlechu ostatních uživatelů. Jejich cena je vyšší vzhledem k potřebě užívat aktivní prvky např. switche, sfp atd. [3]

PON - passive optical network

Tato technologie se postarala o obrovské rozšíření optických sítí mezi koncové uživatele. Díky použití pasivních prvků – deličů (splitterů) došlo k drastickému snížení ceny přípojek na srovnatelnou cenu s cenou klasických metalických rozvodů. Na síti nejsou použity žádné aktivní prvky, z tohoto důvodu je maximální rozdíl ve vzdálenostech koncových zařízení 20 km a je zde třeba vhodným rozložením děličů získat požadovaný útlum. Prozatímní technologie dovoluje připojení až 128 uživatelů, kteří mohou současně komunikovat v obou směrech. [3]

PON sítě využívají mnoho standardů, z nichž nejpoužívanějším je GPON, neboli gigabit PON. Jedná se o první standard umožňující přenosové rychlosti okolo 1 Gbit/s v obou směrech. Šifrování v těchto sítích je volitelné, z čehož vyplývá možnost zneužití. Dalšími standardy pasivních optických sítí jsou APON a BPON, které jsou nejstaršími technologiemi PON. [3]

Bezpečnost APON a BPON

Díky nové metodě šifrování zvané churning, která byla zavedená standardem APON, měla být zajištěna důvěryhodnost dat koncových uživatelů pouze v sestupném směru, avšak vzhledem k velkému počtu chyb není tento druh šifrování bezpečný a koncoví uživatelé mohou být odposlouchávání. Funkce šifry spočívá v mapování 8bit plaintextů na 8bit ciphertexty, přičemž dochází k zašifrování 24bit klíčem, který je aktualizován alespoň jedenkrát za sekundu. Vzhledem k množství přenášených informací až 662 Mbit/s v sestupném směru je poskytnut dostatek dat pro kryptoanalýzu. Další problém spočívá v autentizaci ONU jednotek OLT jednotkou, u které není nutnost hesla spravovat, a tak může dojít k problémům s autentizací, popřípadě k absolutní absenci autentizace. [21]

Bezpečnost GPON

Šifrování dat je v případě GPON volitelné, přičemž se jedná pouze o komunikaci v sestupném směru, a to jen v případě uživatelských dat. Služební zprávy nejsou šifrovány vůbec a lze je tedy v sestupném směru odposlouchávat. V sestupném směru mohou být data šifrována symetrickou šifrou AES, přičemž klíče jsou distribuovány prostřednictvím PLOAM zpráv jako čistý text. Ve vzestupném směru nejsou data šifrována vůbec. Díky mnoha možnostem provedení odposlechu jsme schopni odposlouchávat komunikaci v obou směrech, ač v sestupném směru je komunikace šifrovaná, jsme schopni odposlechnout PLOAM zprávy obsahující šifrovací klíče. Ve vzestupném směru není komunikace šifrována vůbec a lze ji tedy jednoduše odposlechnout celou. Tato možnost představuje velké riziko vzhledem k obsahu těchto zpráv – hesla, platební údaje atp. Tyto bezpečnostní nedostatky řeší novější standarty PON sítí, jako je například XG-PON. [22]

Aktivní zařízení PON sítí

OLT – optical link termination, slouží pro poskytování služeb síťového rozhraní

ONT – optical network termination, je koncové zařízení umožňující využívat služeb přístupové sítě

ONU – optical network unit slouží jako zařízení převádějící optické rozhraní na metalické – „převodník“

3 Únik dat v optických sítích

Existuje spousta možností, kde může dojít k úniku informací. Není lehké tyto možnosti klasifikovat, avšak základní rozdělení může být provedeno následovně. První skupinou jsou útoky, při kterých dojde k výpadku na trase a jsou tedy zaznamenatelné mechanismy na kontrolu sítě. Další skupinou jsou útoky, které nevyžadují změnu optické vláknové infrastruktury, zejména se jedná o různé možnosti odposlechu díky fyzikálním vlastnostem optických vláken.

3.1 Možnosti úniku dat s přerušením vlákna

3.1.1 Vložení optického děliče

Optický dělič pasivně rozděluje záření na určitý počet částí. Pro jeho vložení je třeba trasu rozpojit a do trasy vložit. Tento výpadek je v závislosti na jeho délce velmi jednoduše zjistitelný jak monitoringem sítě na straně poskytovatele, tak nefunkčností služeb na straně uživatelů v případě odposlechu ISP. Toto lze obejít správným načasováním útoku, při nahlášeném nebo náhodném výpadku, kdy dojde k porušení trasy někým jiným. Vložený dělič má velký poměr odkloněného signálu ku tomu dále propuštěnému až 99:1, vložený útlum je tedy velmi malý, což při správné aplikaci je téměř neodhalitelné při měřeních odporu přímou metodou, přičemž u měření metodou OTDR dojde k jednoduchému odhalení. Odposlech optických vláken skrz vložený dělič je velice efektivní a tyto děliče mohou sloužit několik let bez odhalení. Tento typ útoku může mít mnoho variací v závislosti na umístění děliče v trase, kdy existuje možnost dělič vložit za jiné prvky způsobující útlum či zesilující signál, a tak dále snížit šanci na odhalení.

3.1.2 Vložení demultiplexoru

Z podstaty věci tento útok pracuje na podobném principu jako vložení optického děliče. V tomto případě neodkláníme z hlavního vlákna část záření v celém spektru, ale část záření s určitou vlnovou délkou. K realizaci lze využít všechny typy vlnových demultiplexorů, nejjednodušší bude užití demultiplexoru pracujícího s braggovými mřížkami.

3.1.3 Vložení aktivních zařízení

Tato technika replikuje klasický MitM útok a spočívá ve vložení aktivního zařízení mezi 2 jiná mezi sebou komunikující zařízení. Vložené zařízení může být buď optoelektronické.Při vstupu optického signálu je signál převeden na elektrický a

následně analyzován nebo modifikován a poté poslán dál. Nevýhodou je zpoždění signálu oproti nenarušené formě přenosu. Druhou možností je použití optotronického zařízení, ve kterém je optické záření přímo analyzováno. Tato technika je z pohledu odhalitelnosti výhodnější, signál prochází přímo a není tak zpožděn, nedochází tedy k „prodloužení délky trasy“. Při této aplikaci je třeba na výstupu vracet optický signál se stejnou intenzitou jako na vstupu, aby se zamezilo odhalení při měření útlumu přímou metodou. Obě metody jsou odhalitelné měřením pomocí OTDR. [19]

3.2 Možnosti úniku dat bez přerušení vlákna

3.2.1 Fibre tapping

Jedná se o metodu odposlechu bez narušení celistvosti vlákna. Využívá úprav vláken, kde je část záření vyzářena z jádra vlákna a následně zpracována. V závislosti na metodě částečně vkládá do trasy útlum odpovídající poloměru ohybu. Hlavní výhodou při správné aplikaci je mnohdy až relativně nemožná odhalitelnost, na rozdíl od metod kdy je třeba rozpojení trasy, jež bude snadno detekováno. Odhalitelnost pak velmi závisí na množství vloženého útlumu. [18]

Makroohyb

Při dostatečném ohybu optického vlákna může dojít k vyzáření části paprsku mimo jádro, potažmo mimo celé vlákno vlivem překročení mezního úhlu odrazu paprsku. Při instalaci optických vláken je tedy třeba dbát na hodnoty bezpečného poloměru ohybu vlákna udávané výrobcem, přičemž je mezní úhel ovlivněn průměrem vlákna a jeho typem dle standartu ITU-T. Zpravidla by neměl krátkodobě ohyb dosahovat stonásobku průměru vlákna, z dlouhodobého hlediska dvě stě až šesti set násobku průměru vlákna. Tento jev lze využít pro uskutečnění jednoho z nejjednodušších útoků na fyzickou vrstvu optických sítí, při kterém lze odposlouchávat vlákno bez jakéhokoli narušení trasy. Tohoto jevu můžeme využívat i v měřících přístrojích jako jsou optické identifikátory, které detekují provoz na trase. [18]

Mikroohyb

Zahrnuje veškeré ztráty způsobené nedokonalostí vlákna způsobených ve výrobě, jedná se o odchylky v průměru vlákna nebo nerovnosti na hranici jádra a pláště. Dalším působitelem mikroohybů je vnější tlak, který způsobí, že jádro je ohnuto a dochází k podobnému efektu jako u makroohybu. Tyto nedokonalosti mnohou vznikat kdekoli na trase a je vizuálně obtížné je oproti makroohybům odhalit, proto způsobují další útlum na trase. Uniklé záření je možné odposlouchávat, ačkoli vzhledem k množství vloženého útlumu, tedy relativnímu množství uniklého záření, je tato metoda obtížnější. [18]

Evanescentní párování

Při totálním odrazu na hranici dvou prostředí s různým indexem lomu, v tomto případě hranice jádro – plášt dochází ke vzniku evanescentní vlny postupující podél hranice oněch prostředí. Vlna vyzařuje obvykle do vzdálenosti několika set nanometrů. Pokud dojde k odstranění izolace vlákna a části pláště, jsme za velmi specifických podmínek schopni přiložením druhého podobně upraveného vlákna zachytit tyto vlny a odposlouchávat tak komunikaci. Úskalí této metody spočívá v potřebě extrémně přesného přiložení vláken, aby druhé vlákno bylo v dosahu vyzařované evanescentní vlny a bylo schopno ji pojmout, což je v běžných podmínkách poněkud složité. Výhodou této metody je její neodhalitelnost. [18]

Braggovy mřížky

Vytvořením Braggovy mřížky v jádru vlákna jsme schopni odfiltrovat část záření, podobně jako na tomto principu fungující demultiplexer, viz. kap. 2.7, ale na rozdíl od demultiplexeru Braggovy mřížky slouží k odfiltrování určité části záření, které je možné využít k odposlechu. Vytvoření Braggovy mřížky je složitý proces vyžadující použití UV laseru, jehož aplikace v nelaboratorních podmínkách je nadmíru složitá, takže nedochází k častému používání této metody. [18]

3.2.2 Měření zpětného odrazu

Při průchodu záření 2 prostředími s jiným indexem lomu dochází k částečnému odrazu zpět ke zdroji, jedná se o zpětný odraz. Tento jev vzniká zejména na optických konektorech a tvoří značnou část jejich vloženého útlumu. Záření prochází naleštěným koncem ferule směrem ke druhému konektoru a vzniká zde rozhraní vlákno/vzduch/vlákno. Na velikost zpětného odrazu má vliv mnoho faktorů, jako je typ použitého leštění ferulí nebo čistota a celkový stav konektorů. Tento odraz je možné měřit a odposlechnout. [16]

3.2.3 Odposlech přeslechu

Jedná se o nežádoucí jev vznikající na aktivních i pasivních prvcích optických přenosových soustav. Jednou z možností je odposlech WDM na multiplexerech. Žádný multiplexer není ideální, a tak se určitá část sousedních kanálů překrývá a je možné ji odposlechnout. Velikost přeslechu závisí na konstrukci multiplexeru, tedy na vzdálenosti mezi jednotlivými přijímači vlnovodu. Další možností je měření přeslechů na optických přepínačích, které opto-mechanicky přepínají mezi jednotlivými kanály, nejčastěji 1x2 nebo 1x4, kdy je možno odposlouchávat určitou část záření i na neaktivním výstupu. Tento přeslech nevzniká překryvem jednotlivých kanálů, ale nedokonalou izolací mezi jednotlivými výstupy. Část záření uniká i naktivními kanály.

3.2.4 Upravená ONU jednotka

Tento typ útoku může ze všech možností útoku na GPON sítě lákat útočníka asi nejvíce, jedná se ale o velmi složitý proces úpravy FW, který není vždy proveditelný. Běžně fungující jednotka zpracovává data určená pouze pro ni, přičemž ostatní data jsou zahozena. Odhalení upravené jednotky je velmi složitý proces, kdy je předpoklad, že takto upravená jednotka bude mít velmi malý poměr zahozených rámců a také nejnižší chybovost. Tímto způsobem jsme schopni odposlechnout všechna data v sestupném směru, ovšem nejedná se o jediný možný způsob odposlechu a je možné užití i jiných detektorů záření, například napojením na „živá“ ale nepoužívaná vlákna. [20]

3.3 Bezpečnost optických sítí

Jak bylo již několikrát zmíněno, tak přenos velkého množství dat, který je spojen s optickými sítěmi z nich dělá struktury velmi citlivé na poruchy komunikace způsobené vnějšími vlivy nebo samotným selháním prvků. Bezpečná síť by měla zajistit zabezpečení komunikace ve všech ohledech a alespoň nějakou formu řízení kvality služeb. Útoky zmíněné v předešlých sekcích vytvořily velké množství požadavků na NMS, tedy network management systém, který je odpovědný za konfiguraci sítě, výkonnostní inženýrství, řešení poruch a bezpečné fungování sítě. Základním kamenem efektivního NMS v optických sítích je flexibilní robustní systém, který se opírá o časté a přesné měření, a je tedy velmi účinně schopen reagovat na veškeré změny které mohou nastat, například útoky nebo výpadky. [14]

Základní funkce NMS

Řízení zdrojů

Je velmi důležité mít přesné informace ohledně dostupnosti zdrojů za jakýchkoli podmínek, přičemž musí docházet k časté aktualizaci, zejména při navázaní nových spojení nebo jejich výpadku. [14]

Zřizování cest

Při prvotním spuštění by mělo dojít k automatickém objevení veškerých aktivních prvků sítě a tedy k objevení topologie. Pro každý požadavek by měl být systém schopný spočítat nejlepší trasy a vést řízení kvality služeb, proto jsou velmi klíčové informace o dostupnosti zdrojů. [14]

Signalizace

Je třeba mít zřízenou správnou výměnu informací ohledně daných spojení. Sytém musí reagovat na jakoukoli změnu v topologii sítě a být schopen na ně upozorňovat. [14]

Detekce útoku

Při jakémkoli zhoršení signálu, celkovém výpadku služeb, či jiném vzniklém důsledku útoku na optickou síť musí být zjištěna přesná poloha vzniklého „jevu“ a následně určen jeho zdroj a důvod, proč k němu došlo. Po spuštění bezpečnostních mechanizmů musí systém izolovat danou část sítě, na které je útok prováděn a musí dojít k neutralizaci škodlivých účinků v co nejkratším čase. [14]

3.4 Prevence útoků

Rizika a následná poškození optických sítí lze zmírnit, avšak vzhledem k ekonomickým faktorům téměř nikdy zcela vyvrátit, je tedy důležité najít správný kompromis mezi náklady a poskytnutou ochranou. Při stavbě optické sítě je velmi důležité dbát na pečlivé naplánování, kudy vlákna budou vedena, kde budou umístěny aktivní nebo pasivní prvky a jak bude jejich zabezpečení. Jako prevenci před útoky je třeba zabezpečit data různými kryptografickými systémy dle užité technologie optické sítě a velmi dynamicky reagovat na veškeré vzniklé situace odlišné od normálního provozu. Prevence sehrává důležitou roli při posilování odolnosti optických sítí vůči útokům a snížení jejich dopadů. [14]

Fyzické aspekty

Při stavbě sítí je třeba správně volit jednotlivé komponenty. Volbou chráněných optických vláken na exponovaných místech dojde ke zvýšení náročnosti provedení útoků odposlechem (makroohyb). Dalšími vhodnými komponentami mohou být zařízení omezující nadměrný výkon, která ochrání při útocích rušením, nebo používání optických rozvaděčů neužívajících univerzální klíče. [14]

Šifrování dat

Šifrování chrání důvěrnost komunikace a zamezuje odposlechu použitelných informací, nebo alespoň jejich části. [14]

Optická steganografie

Pracuje na principu skrytí komunikace mezi 2 uživateli pod veřejný komunikační kanál. Útočník nezjišťuje probíhající komunikaci daných uživatelů, ale jen tu hlavní. Můžeme tedy docílit vytvoření komunikace velmi odolné oproti odposlechu a rušení. Tuto komunikaci lze zajistit spontánními emisemi z EFDA zesilovačů. Je zřejmé, že tato metoda není aplikovatelná globálně, ale slouží v případě potřeby velmi bezpečné komunikace. [14]

3.5 Detekce a následná reakce na útoky

Detekce útoků je založena na spolehlivých monitorovacích metodách. Je třeba, aby bylo měřeno v optické rovině bez interpretace přenášených dat. Tyto metody mohou vycházet ze statistické analýzy měřených signálů. Mezi nejběžnější metody monitoringu patří použití metody OTDR nebo pilotního tónu. Pilotní tóny jsou speciální signály, které jsou vyhrazené pro detekci přerušení spojení. Mohou být přenášeny společně s pracovními signály na jiné frekvenci. V rámci reakce na útoky by se měl NMS co nejrychleji snažit útok signalizovat a včasně na něj reagovat např. odpojením příslušné části od sítě. Problém s nalezením přesného místa útoku spočívá v možnosti několikanásobných výpadků, které vznikly buď samy nebo cizím zaviněním, kvůli kterému může útočník skrýt pokusy o útok, jež by za normálního provozu vzbudily velký rozruch. V tomto sytému je důležitá souvztažnost mezi výpadky a útoky v každém uzlu sítě, aby byl mechanismus schopen jednotlivé útoky s jistou přesností odhalovat. Funkčnost tohoto algoritmu závisí na NMS, který musí být schopen správně delegovat a zpracovávat provozní zprávy na uzlech sítě a zajistit tak funkčnost. Pokud je nějaký útok detekován je nutné reagovat co nejrychleji a po následném rozboru situace je třeba provést co nejvíce akcí pro následnou minimalizaci rizik. [14]

Nejběžněší možnosti úniků informací z optických vláknových infrastruktur		
název	riziko / závažnost	pravděpodobnost útoku
makroohyb	vzniká často samotným vedením trasy, potřeba užití kvalitního fotodetektoru pro odchyt, samotný výskyt je závažný, významné riziko	vznikají vždy, útok pravděpodobný
mikroohyb	velmi malé množství uniklých informací, těžko zpracovatelné, nezávažné	spíše v laboratorních podmínkách, jinak nepravděpodobný
evanescentní párování	velmi malé množství uniklých informací, těžko zpracovatelné, spíše experimentální, nezávažné	spíše v laboratorních podmínkách, jinak nepravděpodobný
tvorba Braggových mřížek	útok je možný, spíše ale formou vložení MUXu, středně závažné	spíše v laboratorních podmínkách, jinak nepravděpodobný
přeslechy	středně závažné, vznikají nehledě na útočníkovi, nezanedbatelné riziko	vznikají téměř vždy, pravděpodobný
zpětný odraz	středně závažné, vnikají nehledě na útočníkovi význammné riziko	jednoduché odchycení, nutnost zpracování dat dle použité technologie, velmi pravděpodobný
vložení děliče	jednoduché na realizaci, těžko odhalitelné, závažné, významné riziko	velmi pravděpodobný
vložení MUXu	podobný princip jako u vložení děliče, závažné	možný
úprava FW ONU jednotky	velmi závažné, ale obtížná realizace	o realizaci se může pokusit každý koncový uživatel, pravděpodobný

Tab. 3.1: Nejběžnější možnosti úniků informací

4 Praktická část

Praktická část této práce bude zaměřena na realizaci nejběžnějších útoků na optickou vláknovou infrastrukturu včetně aktivních a pasivních zařízení. Zprvu dojde k definici hodnotící strategie závažnosti jednotlivých útoků v rámci analýzy rizik. Bude následovat několik realizací jednotlivých útoků - vložení optického děliče, vytvoření makroohybu, odchyt zpětného odrazu a měření přeslechů na několika druzích zařízení. U každého měření bude provedena analýza rizik dle předešle definovaného hodnocení a následný návrh minimalizace rizik. Poslední část praktické části bude věnována minimalizaci rizik GPON sítí.

4.1 Analýza rizik

Z obecného hlediska je důležité si stanovit, jaká rizika mohou vůbec vzniknout a jaký je stupeň jejich dopadu. K potřebnému stanovení rizik je potřeba vědět co nejvíce informací, počítat s veškerými faktory a scénáři a následně je analyzovat. Tento proces může být velmi zdlouhavý. Důvodem hodnocení rizik je potřeba mít možnost je systematicky porovnat. Díky tomuto porovnání máme jasné měřítko a můžeme začít kalkulovat s tím, jaká rizika jsme schopni podstoupit a jaká nikoli. Následně by měl vzniknout návrh na minimalizaci/eliminaci rizik, která jsme nepodstoupili. Při analýze rizik je vhodné počítat s různými scénáři a provést velmi konkrétní analýzu. [23] U jednotlivých scénářů je hlavní si určit, jak se budou jednotlívé útoky navenek tvářit, jestli dojde k výpadku či nikoli, zda se zvýší celkový útlum na trase, jaké informace jsme schopni získat, jak těžké je útok provést a jak složité je jeho odhalení. Každý z těhto atributů bude bodově ohodnocen a následně dojde ke stanovení, jak je dané riziko kritické a jaký bude mít možný dopad. Velikost dopadu bude záviset na součtu 4 hodnotících kritérií. Maximum 20 bodů, minimum 0 bodů.

Typ útoku a jeho invazivnost	Hodnota
Útok není invazivní - nedojde k rozpojení a nebude vložen útlum	5
Nedojde k výpadku, ale vzroste hodnota útlumu na trase	4
Dojde k výpadku s nepředvídatelnou délkou	3
Dojde k výpadku s předvídatelnou délkou	2
Dojde k výpadku bez obnovení spojení	1

Tab. 4.1: Hodnocení invazivnosti útoku

Typ informací	Hodnota
Veškeré informace jsou nešifrované	5
Část informací je šifrovaných, část nešifrovaných	3
Celá komunikace je šifrovaná	1

Tab. 4.2: Hodnocení druhu odposlechnutých informací

Určení znalostí a vybavení	Hodnota
Není potřeba žádné speciální vybavení nebo schopnosti - útok providitelný laikem	5
Potřeba základního vybavení nebo schopností	3
Potřeba kontrétního vybavení nebo velké znalosti	1

Tab. 4.3: Hodnocení obtížnosti provedení útoku

Způsob odhalení	Hodnota
Neodhalitelný	5
Nezjistitelný měřením, pouze komplexní prohlídkou celé trasy	4
Zjistitelný komplexními metodami monitoringu sítě a měření pomocí OTDR	3
Jednoduše odhalitelný	1

Tab. 4.4: Hodnocení složitosti odhalení

Celkový součet	Stupeň dopadu
1-4	Zanedbatelné riziko
5-8	Drobné riziko
9-12	Nezanedbatelné riziko
13-16	Významné riziko
17-20	Nepřijatelné riziko

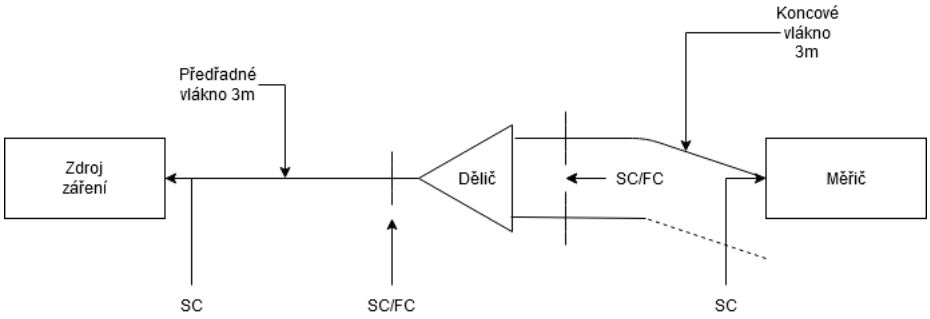
Tab. 4.5: Určení stupně dopadu

4.2 Vložení děliče

Cílem měření je určení útlumu vloženého děliče s poměrem 80:20, 90:10 a 99:1 přímou a nepřímou metodou na vlnových délkách 1310 nm a 1550 nm s následnou analýzou možnosti úniku informací včetně reálné realizace útoku s vytvořením časového odhadu potřebného k útoku. K měření útlumu budou využity dvě metody. Měření pomocí přímé metody a měření pomocí OTDR. Následně proběhne 30 pokusů o zapojení děliče do trasy spojení point-to-point a point-to-multipoint pro zjištění délky výpadku a porovnání mezi jednotlivými typy spojení.

4.2.1 Měření přímou metodou

Měření přímou metodou funguje na principu zjištění, o kolik byl signál oslaben při průchodu trasou. V rámci měření byl použit zdroj záření Exfo FLS-600 a měřič optického výkonu FOPM-102. Jednotlivé děliče byly vybaveny konektory FC, proto bylo zapotřebí použít spojky SC/FC, protože zdroj i detektor mají SC konektory. Mezi každým přepojením byly konektory očištěny. Potřeba čištění byla velmi velká u děličů 90:10 a 99:1, kdy docházelo k razantnímu nárůstu útlumu vlivem nečitot, tyto nečistoty způsobovaly útlum až 0,3 db.



Obr. 4.1: Schéma zapojení při měřní přímou metodou

Vstupní konektor	Výstupní konektor	Útlum udávaný výrobcem [dB]	Naměřený útlum při 1310 nm [dB]	Naměřený útlum při 1550 nm [dB]
P1 - RED	P3-BLUE	1,44	7,21	7,11
P1 - RED	P4-BLACK	7,13	1,56	1,43
P1 - WHITE	P3-BLUE	7,06	1,63	1,58
P1 - WHITE	P3-BLACK	1,28	7,79	7,38

Tab. 4.6: Naměřené hodnoty přímou metodou pro dělič 80:20

Vstupní konektor	Výstupní konektor	Útlum udávaný výrobcem [dB]	Naměřený útlum při 1310 nm [dB]	Naměřený útlum při 1550 nm [dB]
P1 - RED	P3-BLUE	0,68	10,45	9,93
P1 - RED	P4-BLACK	10,58	0,79	0,79
P1 - WHITE	P3-BLUE	10,36	0,68	0,65
P1 - WHITE	P3-BLACK	0,72	10,58	10,20

Tab. 4.7: Naměřené hodnoty přímou metodou pro dělič 90:10

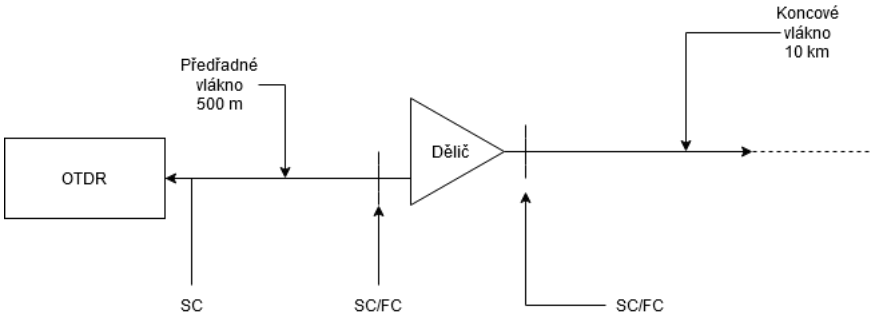
Vstupní konektor	Výstupní konektor	Útlum udávaný výrobcem [dB]	Naměřený útlum při 1310 nm [dB]	Naměřený útlum při 1550 nm [dB]
P1 - RED	P3-BLUE	0,37	22,5	20,66
P1 - RED	P4-BLACK	20,47	0,31	0,26
P1 - WHITE	P3-BLUE	20,43	0,35	0,23
P1 - WHITE	P3-BLACK	0,33	21,91	20,14

Tab. 4.8: Naměřené hodnoty přímou metodou pro dělič 99:1

4.2.2 Měření metodou OTDR

Měření metodou OTDR pracuje na principu kalkulace s hodnotami Rayleighova rozptylu, kdy je část rozptýleného záření odražena zpět a následně analyzována. Také pracuje s hodnotami Fresnelova odrazu, který vzniká na hranicích dvou prostředí s odlišnými změnami indexu lomu, přičemž s narůstající vzdáleností je paprsek tlumen. Tyto informace jsou následně vyhodnoceny a je vytvořena křivka na které lze zjistit veškeré iregularity na trase a jejich vzdálenosti (sváry, děliče,...). [3] Při měření optického děliče metodou OTDR je třeba měřit ve vzestupném směru, jinak by došlo k změření celkového útlumu děliče, protože by došlo ke sečtení hodnot Rayleighova rozptylu na všech výstupech.

K měření bylo použito OTDR Atomo wawe SOT-A80, předřané vlákno délky 500 m s konektory SC, jednotlivé děliče, spojky SC/FC a 10 km dlouhé koncové vlákno. Konektory byly pravidelně čištěny stejně jako u předchozího měření.



Obr. 4.2: Schéma zapojení při měřní pomocí OTDR

Vstupní konektor	Výstupní konektor	Útlum udávaný výrobcem [dB]	Naměřený útlum při 1310 nm [dB]	Naměřený útlum při 1550 nm [dB]
P1 - RED	P3-BLUE	1,44	7,28	6,15
P1 - RED	P4-BLACK	7,13	1,72	1,70
P1 - WHITE	P3-BLUE	7,06	1,63	1,56
P1 - WHITE	P3-BLACK	1,28	7,09	5,77

Tab. 4.9: Naměřené hodnoty metodou OTDR pro dělič 80:20

Vstupní konektor	Výstupní konektor	Útlum udávaný výrobcem [dB]	Naměřený útlum při 1310 nm [dB]	Naměřený útlum při 1550 nm [dB]
P1 - RED	P3-BLUE	0,68	10,42	9,85
P1 - RED	P4-BLACK	10,58	0,81	0,77
P1 - WHITE	P3-BLUE	10,36	0,71	0,64
P1 - WHITE	P3-BLACK	0,72	10,86	10,09

Tab. 4.10: Naměřené hodnoty metodou OTDR pro dělič 90:10

Vstupní konektor	Výstupní konektor	Útlum udávaný výrobcem [dB]	Naměřený útlum při 1310 nm [dB]	Naměřený útlum při 1550 nm [dB]
P1 - RED	P3-BLUE	0,37	18,35	15,90
P1 - RED	P4-BLACK	20,47	0,37	0,28
P1 - WHITE	P3-BLUE	20,43	0,39	0,36
P1 - WHITE	P3-BLACK	0,33	18,31	15,35

Tab. 4.11: Naměřené hodnoty metodou OTDR pro dělič 99:1

4.2.3 Měření časové náročnosti útoku

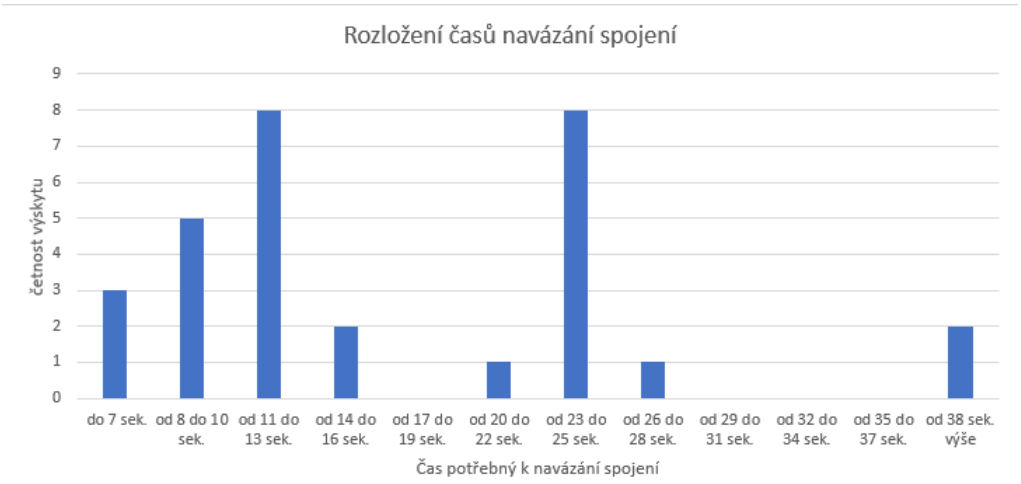
Tato část je zaměřena na určení času potřebného pro uskutečnění útoku. Scénář počítá s tím, že útočník vkládá dělič na místa, kde je možné vlákno rozpojit díky již existujícím konektorům, například u aktivních nebo pasivních prvků, jako je switch nebo zesilovač. Další podobnou možností je umístění k jiným děličům. Může se jednat o rozvodnou bednu ve sklepě domu, na kterou je napojena další domovní infrastruktura.

Point-to-point

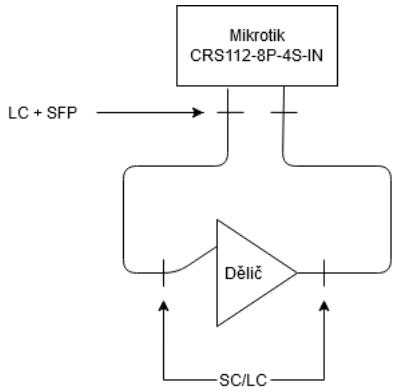
V rámci měření bylo zapotřebí zajistit stbilní měření časových oken - výpadků. K tomuto měření byl použit Mikrotik CRS112-8P-4S-IN, který má 4 SFP moduly. Díky komplexnosti jeho systému jsme schopni přesně zobrazit, na jak dlouhou dobu došlo k výpadku, a to přímo na fyzické vrstvě. Spliter byl zapojen SC/FC spojkou a LC/SC patchcordem na obou stranách. Bylo provedeno celkem 30 měření, následně spočten aritmetický průměr a medián. Dle výsledků byl stanoven potřebný čas k uskutečnění útoku, který odpovídal 2,9 sekundám v případě aritmetického průměru a 3 sekundám, jakožto střední hodnotě.

GPON

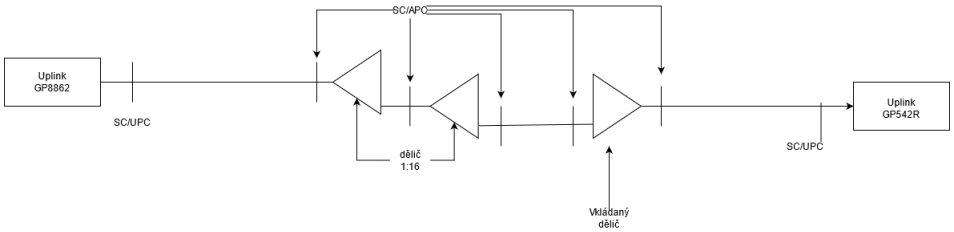
Pro možnost srovnání proběhlo další měření časové náročnosti na existující GPON síti. Při měření byly zaznamenávány 2 časy. Prvním z nich je délka trvání samotného přepojení, jehož čas by měl být podobný jako v předchozím měření. Druhým časem je celkový čas než došlo k obnovení spojení mezi OLT a ONU. Celkem proběhlo 30 měření, ze kterých vyplynula obrovská rozdílnost v jednotlivých výsledcích, kdy maximální rozdíl mezi naměřenými hodnotami byl až 37 sekund. Vzhledem k této rozdílnosti nelze stanovit pravděpodobnou délku výpadku.



Obr. 4.3: Graf naměřených hodnot GPON



Obr. 4.4: Schéma zapojení při měření časů útoku - P2P



Obr. 4.5: Schéma zapojení při měření časů útoku - GPON

4.2.4 Analýza rizik vložení děliče

V tomto konkrétním případě mohou nastat 2 scénáře, vložený dělič bude vložen do aktivní optické sítě, veškerá data budou šifrována a bude zde pravděpodobně striktně nastavený monitoring. Jedná se o nejlepší možný scénář. Na druhé straně může dojít ke vložení děliče do pasivní sítě ve vzestupném směru hned za již existující dělič. Odhalení bude složitější, pokud nedojde k překonání hranice maximálního útlumu a veškerá data budou nešifrována. Zde se jedná o nejhorší možný scénář. V případě první možnosti je skóre 9 (2-1-3-3), toto riziko je tedy nezanedbatelné, vzhledem k šifrování je šance na zneužití uživatelských dat velmi malá. V případě druhého scénáře bude hodnota 15 (3-5-3-4), toto riziko je tedy významné a může dojít k jednoduchému zneužití přenášených dat kvůli absenci šifrování.

point-to-point celkový čas [s]	GPON čas zapojení [s]	Gpon celkový čas [s]	Gpon čas spojení [s]
7	19	4	15
2	10	4	6
2	31	5	26
4	31	6	25
2	15	4	11
3	20	8	12
3	27	6	21
3	31	7	24
4	14	5	9
2	47	4	43
3	17	4	13
3	12	6	6
2	17	7	10
3	13	4	9
3	15	8	7
4	30	6	24
4	16	5	9
2	31	6	25
2	45	4	41
2	17	5	12
3	15	4	11
2	12	4	8
3	31	7	24
3	29	6	23
2	19	4	15
3	20	8	12
4	18	5	13
3	17	4	13
2	31	7	24
3	30	5	25

Tab. 4.12: Čas potřebný k vložení děliče

4.2.5 Minimalizace rizik

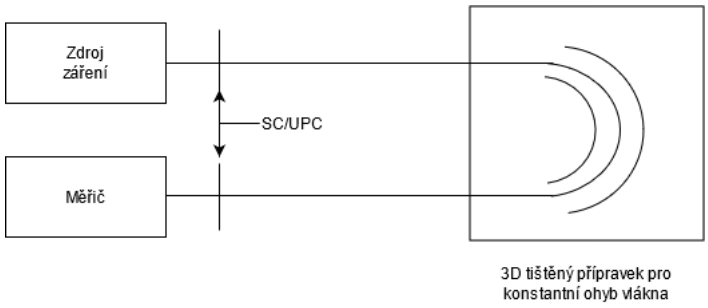
Z naměřených hodnot vyplynulo, že je nejvýhodnější použití děliče 90:10 nebo 99:1 kvůli minimálnímu vloženému útlumu do trasy. V rámci monitoringu sítě by měly být hlášeny veškeré změny útlumu nad 0,3 dB. Z hlediska pravděpodobné změny útlumu, která by teoreticky za normálních provozních podmínek ani neměla nastat, přičemž z praktického hlediska k ní může dojít např. jiným uložením vláken do kazety po přidávání dalšího spojení, avšak hodnoty těchto útlumů dosahují hodnot maximálně jednotek desetin decibelu. Dále je třeba měřit LINK UP/DOWN pomocí SNMP či jiných metod managementu sítě a upozorňovat na všechny výpadky, zejména ty podezřelé, tedy ty s délkou do 5 sekund. Je velmi důležité umět poukázat na vzájemnou provázanost dvou výše zmíněných jevů, dojde-li k náhlému a velmi rychlému výpadku, který nemá absolutně žádné reálné odůvodnění a následně potom k nepatrnému vzrůstu útlumu na trase, je třeba aby byl systém schopen na tyto scénáře upozorňovat nebo aby alespoň informoval správce způsobem, který výrazně napomůže odhalení. U GPON sítí by bylo dobré, aby byly hlídány útlumy na jednotlivých koncových zařízeních a "podezřelé"- z měření vyplývající časy výpadku. Dalším důležitým faktorem je celkové zapezpečení přístupu cizích osob k infrastruktuře, tedy aby došlo k minimalizaci extistence míst, kde je možné útok uskutečnit. Nejdůležitějším nástrojem pro minimalizaci rizik je šifrování veškerého provozu.

4.3 Měření útlumů způsobených makroohybem

Cílem měření bylo stanovit vliv velikosti makroohybu na útlum optických vláken. Pro měření bylo zvoleno vlákno kategorie G.652. a 2 schémata zapojení pro možnost porovnání hodnot. Jako první proběhlo měření přímou metodou a jako druhé měření za pomoci G-PON OLT a jeho vnitřních statistik jednotlivých připojených zařízení. Ohybů vlákna bylo docíleno přípravkem s drážkami jednotlivých poloměrů vytištěným na 3D tiskárně, do kterého bylo vkládáno samotné optické vlákno pouze s primární ochranou.

4.3.1 Měření přímou metodou

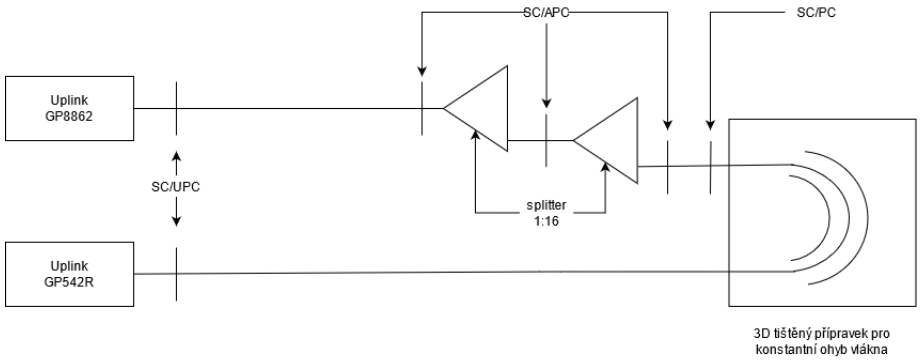
V obou případech byl pro konstantnost měření použit HUAWEI GPON-OLT SFP modul zapojený do optického převodníku tp-link MC220L a měřák optického Noyafa DXP-40D, obě tyto zařízení disponují SC konektory.



Obr. 4.6: Schéma zapojení při měření útlumu přímou metodou

4.3.2 Měření pomocí G-PON OLT

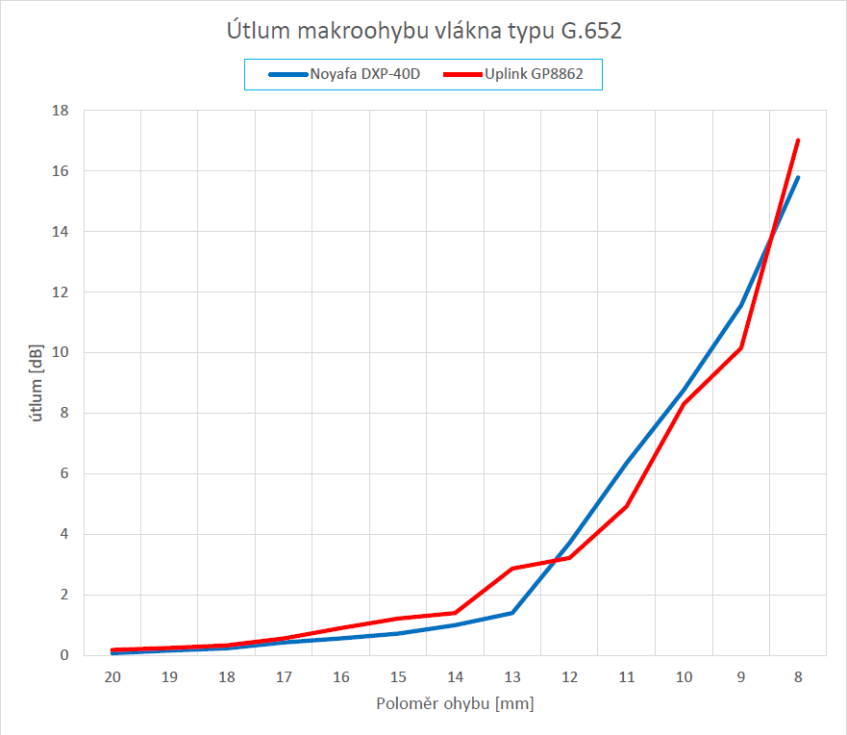
Pro možnost porovnání předchozích hodnot byla využita funkční G-PON síť se stejným SFP modulem jako v prvním měření, kdy v roli OLT byla použita OLT jednotka Uplink GP8862 s koncovým zařízením v podobě Uplink GP542R. OLT jednotka umožňuje zobrazovat hodnoty útlumů na jednotlivých koncových zařízeních, a tak je možné odečíst útlum vložený makroohybem. Aby bylo měření uskutečnitelné, bylo potřeba vložit do trasy 2 děliče s poměrem 1:16 pro získání hodnot útlumu na kterých jsou schopna se jednotlivá ONT spojit s OLT.



Obr. 4.7: Schéma zapojení při měření útlumu za pomocí OLT jednotky

	Noyafa DXP-40D	Uplink GP8862 + GP542R	
Poloměr ohybu [mm]	Odečtený útlum [dB]	Celkový útlum [dB]	Odečtený útlum [dB]
20	0,07	18,448	0,178
19	0,16	18,518	0,248
18	0,23	18,602	0,332
17	0,42	18,828	0,558
16	0,56	19,172	0,902
15	0,71	19,486	1,216
14	0,99	19,666	1,396
13	1,39	21,136	2,866
12	3,71	21,488	3,218
11	6,35	23,188	4,918
10	8,76	26,576	8,306
9	11,55	28,420	10,15
8	15,78	35,277	17,007

Tab. 4.13: Měření útlumu makroohybu



Obr. 4.8: Graf naměřených hodnot útlumu

4.3.3 Analýza rizik makroohybů

Hodnodnocení závažnosti útoku silně závisí na druhu konkrétního vlákna a typu sítě. Existuje předpoklad, že vlákna typu G.652 budou užity hlavně v WAN/MAN PTP sítích vzhledem k nulové disperzi na vlnové délce 1310 nm. Z toho lze předpokládat, že věškerá data budou šifrována a v rámci sítě bude zřízen silný monitoring. Silnou stránkou tohoto útoku je proveditelnost nezávislá na místě. Dle zkušeností z měření může tento typ útoku napáchat spíše více škody než užitku kvůli nutnosti zbavení se veškerých ochran vlákna bez jeho přerušení. Dalším možným problémem je potřeba použití velmi citlivého detektoru pro odchycení záření, které opustilo vlnovod. Lze tedy konstatovat, že tento typ útoku považujeme spíše za teoretický či laboratorně experimentální. V rámci jednotlivých kategorií hodnocení by získal skóre 10 (5-1-5-1), přičemž je ale potřeba zmínit, že množství získatelných dat je velmi limitováno samotným útlumem ohybu.

4.3.4 Minimalizace rizik

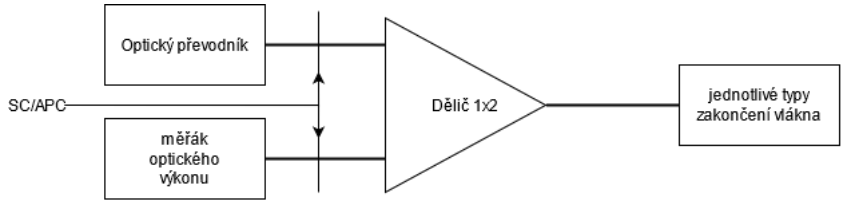
Z podstaty věci by mělo být optické vlákno položeno co nejpříměji s konstantními ohyby velkých poloměrů pro minimalizaci útlumu trasy. Zároveň by mělo být jakýmkoli způsobem chráněno před vnějšími vlivy, včetně vlivu útočníka. Vzhledem k možnosti uskutečnit útok kdekoli na trase je důležité minimalizovat možnost přístupu útočníka k jakékoli části infrastruktury, kde je tento typ vlákna použit a zajistit účinné šifrování veškerého provozu. Zároveň by bylo vhodné monitorovat jakékoli větší a náhodně vznikající změny útlumu trasy nad 3 dB v rámci monitoringu sítě. Je možné, že se útočník o útok pouze pokusí a ač bude neúspěšný, je třeba dané místo prověřit a trasu zabezpečit. V místech kde jsou vlákna přístupnější, například u technologie FTTH u koncových zákazníků, je vhodné použít vlákna s větší odolností vůči ohybům (G.657).

4.4 Měření zpětného odrazu

Toto měření zkoumá vliv použitých konektorů na hodnoty zpětného odrazu v GPON sítích. Tato metoda odposlechu může být využita při útoku na GPON síť a nešifrovanou komunikaci u vzestupného směru. Šifrování za pomoci AES je pouze volitelnou nadstavbou a v mnoha případech tedy není použito, což může vést k pokusům o útok tímto způsobem.

4.4.1 Průběh měření

K měření byl využit optický převodník tp-link MC220L s GPON SFP modulem Huawei, měřák optického výkonu Noyafa DXP-40D, optický dělič s poměrem 1x2 a konektory SC/APC a SC/UPC. Je důležité si uvědomit, že signál v sestupném směru je přenášen na vlnové délce 1490 nm. Signál z koncového zařízení je vysílán na vlnové délce 1310 nm a při odchytu zpětného odrazu by musel být za pomoci např. Braggových mřížek odfitrován.



Obr. 4.9: Schéma zapojení při měření hodnot zpětného odrazu

Druh zakončení	Naměřený útlum [dBm]
Zapojený SC/APC	-63,99
Nezapojený SC/APC	-52,87
Zapojený SC/UPC	-47,34
Nezapojený SC/UPC	-41,73
Vlákno bez konektoru	-27,57

Tab. 4.14: Měření zpětného odrazu

4.4.2 Analýza rizik zpětného odrazu

Tento druh útoku bude uskutečňován zejména v pasivních sítích, kdy velmi pravděpodobně bude vzestupný směr nešifrovaný. K provedení bude ale třeba odfiltrovat sestupný směr od vzestupného - odraženého směru a následné zesílení. Tento útok je velmi pravděpodobně neodhalitelný. V rámci hodnocení by tento typ útoku byl ohodnocen 16 body (5-5-1-5) v případě nešifrovaného vzestupného směru a 12 body (5-1-1-5) v případě šifrovaného vzestupného směru. Riziko je tedy významné ač jednoduše minimalizovatelné.

4.4.3 Minimalizace rizik zpětného odrazu

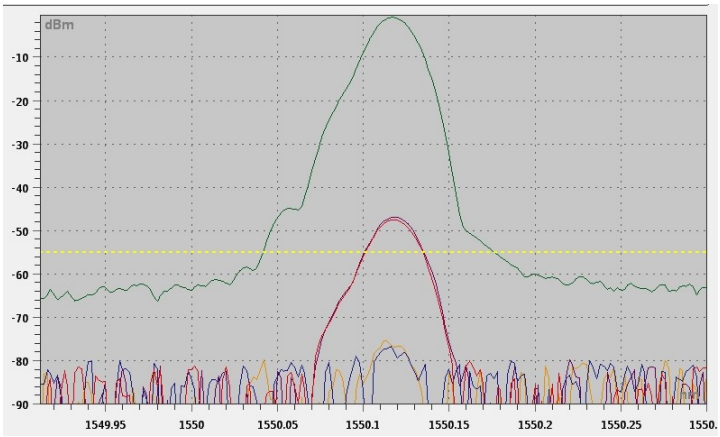
Tento útok je náročný na vybavení - útočník musí nějakým způsobem oddělit odražený vzestupný signál od sestupného a také jej zesílit. Avšak tento typ útoku je pravděpodobný a je vhodné rizika v plné míře minimalizovat. Dále je třeba uvažovat, že data nebudou přicházet pouze od jednoho koncového zařízení, což zhorší možnost odposlechu konkrétních zařízení. Nejlepším způsobem je zavedení šifrování dat symetrickou šifrou AES, která je ve standardu nepovinná - tento nedostatek řeší novější verze standardu, které přímo z GPON vycházejí. Dalším způsobem je minimalizace možnosti přístupu útočníka k pasivním prvkům infrastruktury či k zakončení jednotlivých linek - typicky jsou to volná nachystaná vlákna na chodbě domu, která ještě nebyla zavedena ke koncovým uživatelům. Tento problém vyřeší "umrtvení"vláken nezapojením do děliče. Bohužel nejde zabránit scénáři, kdy útočník bude jedním z již připojených uživatelů, ale tuto možnost lze opět pokrýt šifrováním dat.

4.5 Přeslechy vlnových multiplexů

Cílem měření je provedení spektrální analýzy a změření útlumů přeslechů jednotlivých komponent umožňujících využití vlnového multiplexu, který slouží k navýšení přenosové kapacity přenosového média, díky přenosu na více vlnových délkách. Vlivem neideálních charakteristik jednotlivých komponent může docházet k přeslechům mezi jednotlivými výstupy nebo kanály.

4.5.1 Spektrální analýza přeslechů u DWDM AWG MUXu

Při tomto meření bude stanoveno, jak velký přeslech vzniká na sousedních kanálech. K měření byl použit zdroj záření od PurePhotonics s přesně nastavitelnou vlnovou délkou a výkonem vyzařování, šesnáctikanálový DWDM AWG MUX - kanály 26-41 dle ITU a spektrometr Yenista optics OSA20. Vstupní signál byl vysílán na vlnové délce 1550,12 nm - odpovídající kanálu 9. Následně došlo k změně vlnové délky zdroje záření odpovídající vedlejším kanálům - 7, 8, 10 a 11.

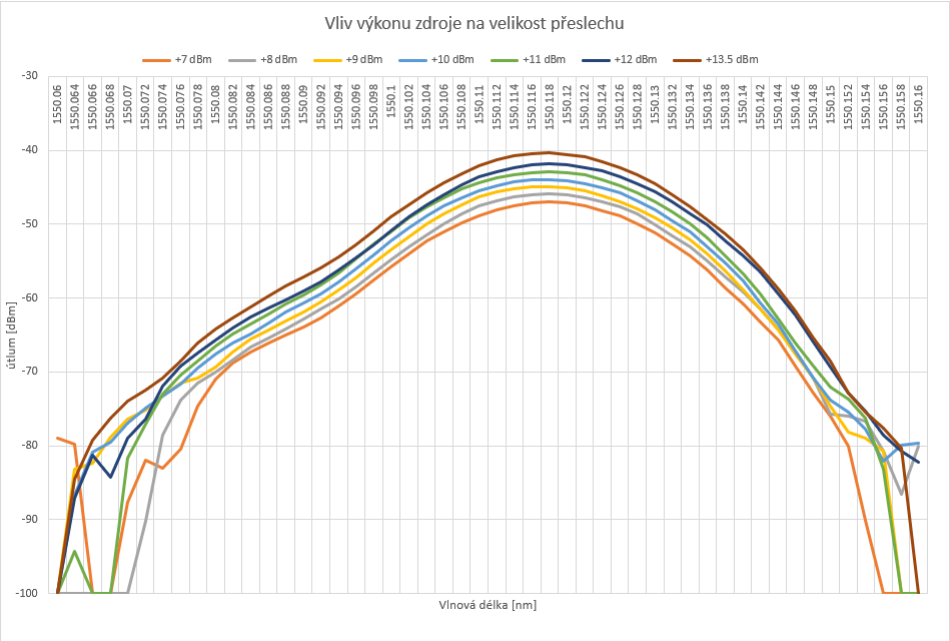


Obr. 4.10: Přeslechy jednotlivých kanálů

Ze spektrální analýzy můžeme usuzovat, že přeslechy na vedlejších kanálech mohou vznikat. Zelená křivka označuje přímý výstup. Červená a fialová pak přeslech z přímo vedlejších kanálů (8 a 10), modrá a žlutá pak přeslech z ob jedno vedlejších kanálů (7 a 11). U sousedních kanálů dosahoval přeslech ohodnot okolo -47 dBm, konkrétně -46,768 dBm u 8. kanálu a -47.261 v případě 10. kanálu. Přeslech z druhé dvojice je zaznamenatelný, ale jeho velikost je tak malá, že možnost zpracování daného signálu je minimální.

4.5.2 Vliv síly vstupního signálu na velikost přeslechu u DWDM AWG MUXu

Díky možnosti nastavení vysílacího výkonu zdroje záření od +6 dBm do +13,5 dBm můžeme ověřit, jakou závislot má výkon zdroje záření na velikost přeslechu. Přeslech byl měřen ze sousedního kanálu 8 na kanál 9 odpovídající vlnové délce 1550,12 nm. Z výsledků měření můžeme pozorovat, že je zde lineární závislost a velikost přeslechu se pohybuje okolo -40 dBm.



Obr. 4.11: Graf závislosti vstupního výkonu na velikosti přeslechu

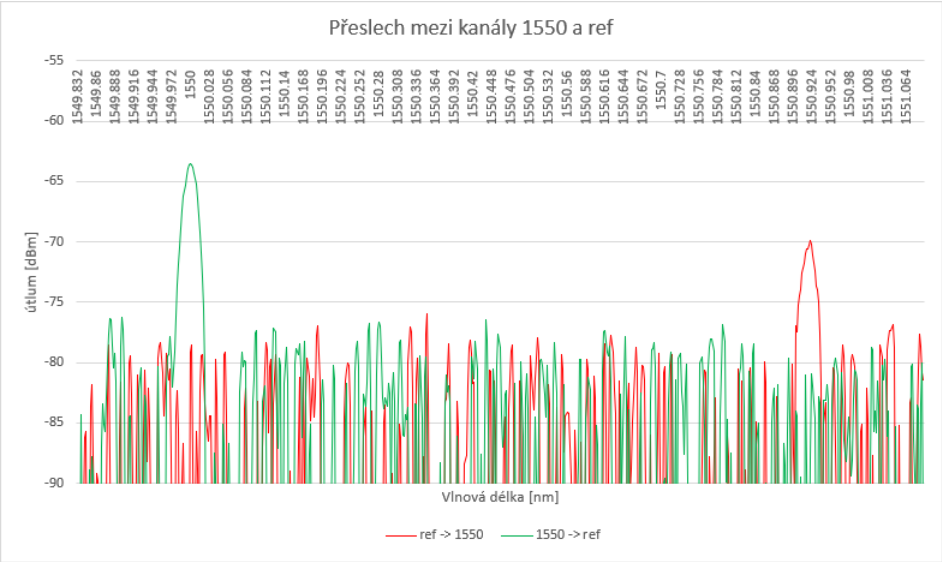
Naměřená hodnota útlumu [dBm] při vlnové délce 1550.12 nm						
+7	+8	+9	+10	+11	+12	+13.5
-47.096	-46.056	-45.104	-44.105	-43.067	-41.984	-40.519

Tab. 4.15: Hodnoty přeslechů u jednotlivých úrovní vstupního výkonu

4.5.3 Spektrální analýza 1x2 CWDM MUXu

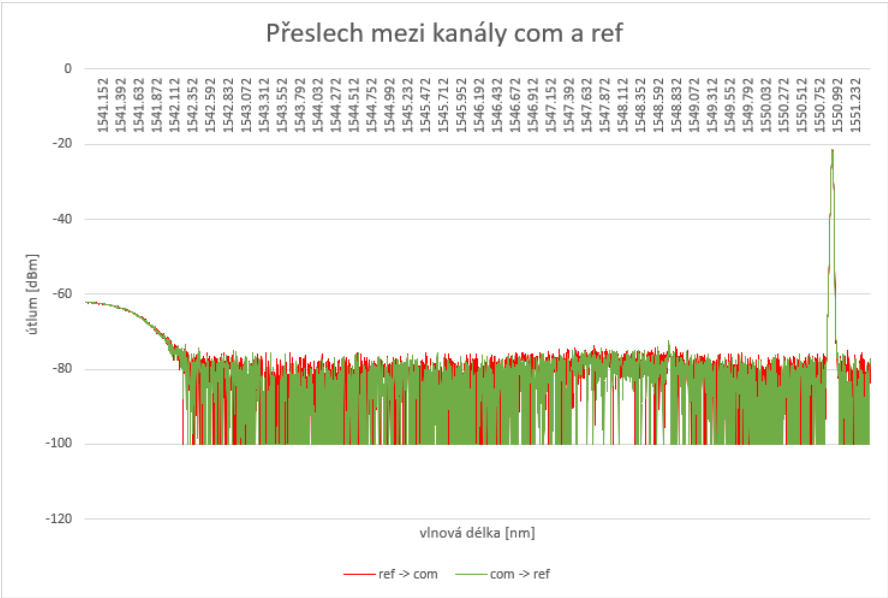
V tomto měření bude provedena komplexní analýza chování vstupujícího záření u všech kombinací vstupů a výstupů CWDM MUXu s jedním vstupem pro druhou nosnou vlnovou délku z rozsahu 1544 nm až 1556 nm (dle inspection sheetu) a zdali se i u těchto pasivních komponent vyskytují přeslechy mezi jednotlivými výstupy. Velikost vysílacího výkonu byla nastavena na +6 dBm.

Na následujícím grafu je vidět vznik přeslechu mezi kanály ref, který slouží pro vložení druhého záření a 1550 sloužící jako hlavní vstup pro původní vlnovou délku. Je zřetelné, že dochází k přeslechu, ač s hodnotami blízko hodnot šumu. Pokud by nastala situace útoku, kdy se útočník pokusí odfitrovat druhou vlnovou délku na původním kanále, směrem zpět od Muxu, musel by použít podobné pasivní zařízení a následně zesilovač. Vzhledem k hodnotě vloženého útlumu z kanálu COM -> ref (viz. obr. 4.13) lze usuzovat, že tento typ útoku je téměř v praxi nerealizovatelný, ač teoreticky možný v laboratorních podmínkách.



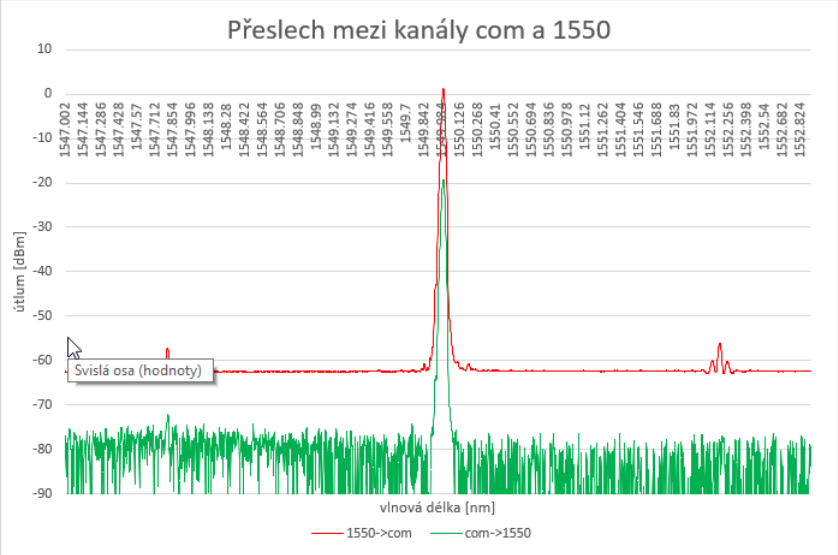
Obr. 4.12: Graf hodnot útlumu přeslechů DWDM muxu (1550, ref)

U tohoto grafu je viditelná standardní funkčnost odfitrování druhé nosné vlnové délky. Pozorujeme poněkud velké hodnoty vloženého útlumu, kdy hodnota na výstupu dosahovala -21,305dBm u směru ref->COM a -21,371 ve směru opačném, což při vstupu +6 dBm a odečtení vloženého útlumu konektorů umisťuje hodnotu vloženého útlumu do rozmezí mezi 26 - 27 dB.



Obr. 4.13: Graf hodnot útlumu přeslechů DWDM muxu (com, ref)

Tento graf znázorňuje běžný přenos mezi kanály 1550 a COM. Zde lze pozorovat rozdílný vložený útlum v závislosti na směru (MUX/DEMUX). Hodnota vloženého útlumu ve směru 1550 -> COM je minimální - hodnota na výstupu 1,193 dBm, což odpovídá vloženému útlumu okolo 4dB. V druhém směru dosahovala hodnota -19,275 dBm a vložený útlum byl podstatně větší. Z toho vyplývá, že tento konkrétní CWDM MUX funguje mnohem lépe jako MUX, tedy pro vkládání druhé vlnové délky, než pro rozdělování. Dále lze pozorovat výchylky na vlnových délkách 1550 +-2,184*n nm. Pokud by došlo ke špatnému zvolení druhé nosné vlnové délky blízko těchto hodnot, mohlo by docházet k negativnímu ovlivňování.



Obr. 4.14: Graf hodnot útlumu přeslechů DWDM muxu (1550, com)

4.5.4 Analýza rizik přeslechů MUX

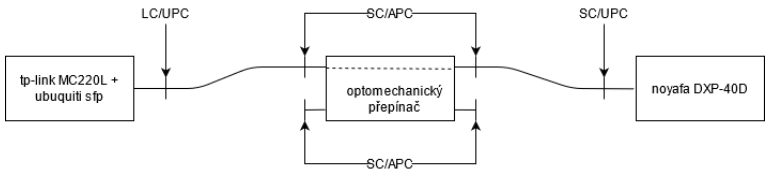
Co se týče přeslechů u multiplexerů, existuje veliká pravděpodobnost, že veškerá komunikace bude šifrována vzhledem ke způsobu použití těchto zařízení, která slouží pro navýšení přenosové kapacity, budou tedy velmi často použita v silně exponovaných sítích. Není zde nutnost vkládání dalších zařízení či rozpojení trasy, ale velmi pravděpodobně bude třeba signál zesílit. Na bodové škále by přeslechy multiplexerů získaly 12 bodů (5-1-1-5), což odpovídá nezanedbatelnému riziku a přesně tak by k němu mělo být přistupováno. Je nutné podotknout, že ač je útok neodhalitelný, existuje o jeho existenci velké povědomí a bude tak snaha o minimalizaci přeslechů.

4.5.5 Minimalizace rizik přeslechů MUX

V předchozích měřeních bylo dokázáno, že u vlnových multiplexerů dochází ke vzniku přeslechů a že závislost mezi velikostí přeslechu a vstupního výkonu je lineární. Hlavním způsobem, jak zamezit odposlechu, či samotnému vzniku přeslechů je zajistit, aby byly vznikající přeslechy co nejmenší. Toho lze docílit zvolením nejmenšího možného vysílacího výkonu a volbou co nejkvalitnějších komponent, které disponují mnohem lepší izolací jednotlivých kanalů.

4.6 Přeslechy optomechanického přepínače

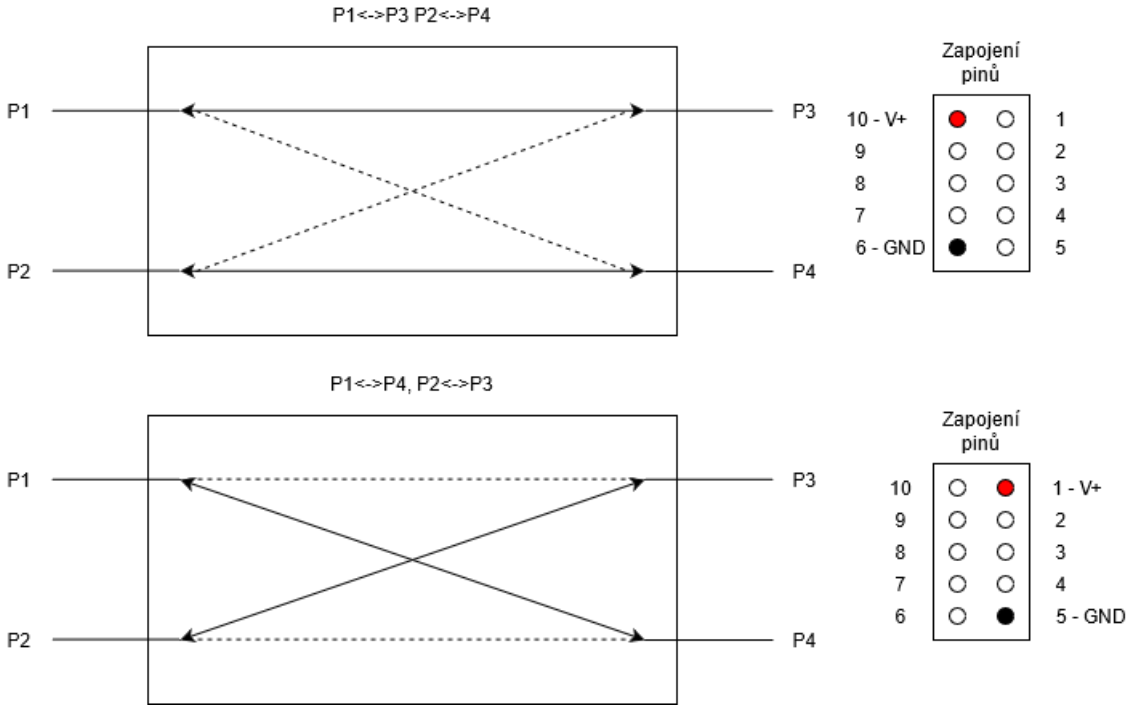
Optomechanický přepínač je druh aktivního zařízení, které dokáže přesměrovat optický signál mezi 2 výstupy za pomoci mechanického přepnutí, které se provádí různým zapojením jednotlivých pinů. Cílem meření bylo ověřit, že tyto komponenty mají velmi nízky vložený útlum a hodnoty přeslechu. K měření byl použit optický převodník tp-link MC220L s SFP modulem Ubiquiti pracující na vlnové délce 1550 nm, měřák optického výkonu Noyafa DXP-40D s citlivostí +10 až -70 dBm a optomechanický přepínač 2X2 od výrobce FS, který byl zapojen do nepájivého pole a pomocí 10cm dupont M-M jumperů přepínán.



Obr. 4.15: Schéma zapojení při měření přeslechů optomechanického přepínače

Při 1550 nm	Udávaný vložený útlum [dB]	Naměřený vložený útlum [dB]
P1-P3	0,96	0,65
P1-P4	1,01	0,82
P2-P4	0,59	0,89
P2-P3	0,71	0,99

Tab. 4.16: Hodnoty vloženého útlumu optomechanického přepínače



Obr. 4.16: Zapojení optomechanického přepínače

Z měření vyplynulo, že vložený útlum z prvního na třetí a čtvrtý kanál byl nižší než hodnoty udávané výrobcem, u druhého kanálu na třetí a čtvrtý byl vložený útlum o zhruba 0,3 dB vyšší než udávaný. Co se týče naměřených odposlechů, nebyly zjištěny žádné na jakékoli dvojici zbylých kanálů, než kterými procházel signál. Je nutné podotknout, že dle výrobce měl být útlum přeslechů menší než 55 dB, kdy u podobných přepínačů od jiných výrobců jsou udávány hodnoty přeslechů až méně než 70 dB a citlivost měřáku optického výkonu sahala na hranici -70 dB, takže zde existuje možnost tvorby přeslechu, ale velmi malého. Lze tedy konstatovat, že tyto optomechanické přepínače se řadí spíše na bezpečnější část spektra, přičemž jejich asi největší slabinou je možnost lokální úpravy toku paprsku, kdy útočník může snadno přepínat a cílit zejména na výpadky vlivem útoků typu odepření služby (DoS).

4.6.1 Analýza rizik optomechanického přepínače

Vzledem k téměř nevznikajícím přeslechům je tento typ útoku na informace velmi nepravděpodobný, bude mít tedy spíše destruktivní charakter a na bodové škále ohodnocen 8 body (1-1-5-1).

4.6.2 Minimalizace rizik optomechanického přepínače

Z výsledků měření vyplynulo, že útoky na tento typ zařízení nebudou zaměřeny na získání informací, ale na dostupnost služeb. Je třeba maximalizovat nemožnost přístupu k těmto komponentám v rámci infrastruktury popř. znemožnit útočníkovi přepínat mezi jednotlivými výstupy.

4.7 Minimalizace rizik PON sítí

Část předešlých měření se zabývala prověřováním jednotlivých možností útoku na pasivní optické sítě. Tato část je věnována zajištění bezpečnosti pasivních sítí, konkrétně u standardu GPON. Pro realizaci korektního nastavení a návrh minimalizace rizik byla využita GPON OLT jednotka Siemens surpass hix 5750 a koncová zařízení v podobě ONU Nokia/Siemens H640V-G25E. Je důležité zmínit, že nastavení ONU jednotek se provádí skrz OLT, což značně omezuje pokusy o úpravu FW a přepnutí ONU jednotek do promiskuitního režimu, či k jakékoli jiné úpravě, což zvyšuje bezpečnost tohoto systému.

4.7.1 Konfigurace OLT

Konfigurace je vykonávána připojením RJ45 to serial do consolového portu s použitím převodníku na USB a následném spuštěním putty -> serial conection. Pro připojení je zapotřebí nastavit bauld rate na 38400 bit/s. Následující proces probíha v command line interface. Komunikace je možná i skrz Telnet, který ale není bezpečný vzhledem k absenci šifrovaní. Dalším velmi důležitým krokem ke zvýšení bezpečnosti je nastavení bezpečných přihlašovacích údajů. [22]

4.7.2 Přidání zařízení

U některých jednotek OLT je třeba zařízení manuálně přidávát, což je i případ toho konkténího OLT, aby došlo k autentizaci jednotlivých ONU. V tomto případě zadáváme několik potřebných údajů včetně adresy, podle které budeme k zařízení v rámci konfigurace přistupovat, typu jednotky, sériového čísla nebo hesla. Pro bezpečnou komunikaci je nejdůležitější hodnota Security mode, která udává zda-li je komunikace šifrována. V případě hodnoty 0 je šifrování vypnuto, v případě hodnoty 1 je šifrování zapnuto. Šifrování probíha symetrickou šifrou AES s délkou klíču 128 bitů, což vzhledem k pravidelné výměně klíčů každých 5 minut je dostačující délka. Dalším důležitým faktorem je správné nastavení hesla potřebného pro následnou konfiguraci daného zařízení. [22]

Příkaz pro přidání ONU:

GPON-OLT-SIEMENS(config)create onu g25a-001 1/1/1 xxx xxx xxx - další zadávané atributy

4.7.3 Konfigurace a práce s koncovou jednotkou

V případě potřeby konfigurace ONU jednotky je třeba k ní přistupovat pomocí její adresy. Samotné ONU má pak i vlastní adresy jednotlivých rozhraní (eth1-eth4). Tento způsob je poněkud archaický, v nejnovější ONU/ONT jsou vybaveny plnohodnotným grafickým uživatelským rozhraním přístupným z webového prohlížeče, nicméně díky tomuto způsobu nemají koncoví uživatelé přístup ke konfiguraci koncových jednotek, z bezpečnostního hlediska je to částečně výhodné, ale na druhou stranu uživatelsky nepřívětivé. [22]

Samotná konfigurace je velmi intuitivní, po zadání otazníku je zobrazena uživateli nápověda, pomocí které dokáže jednoduše veškerá zařízení konfigurovat a zobrazovt potřebné informace.

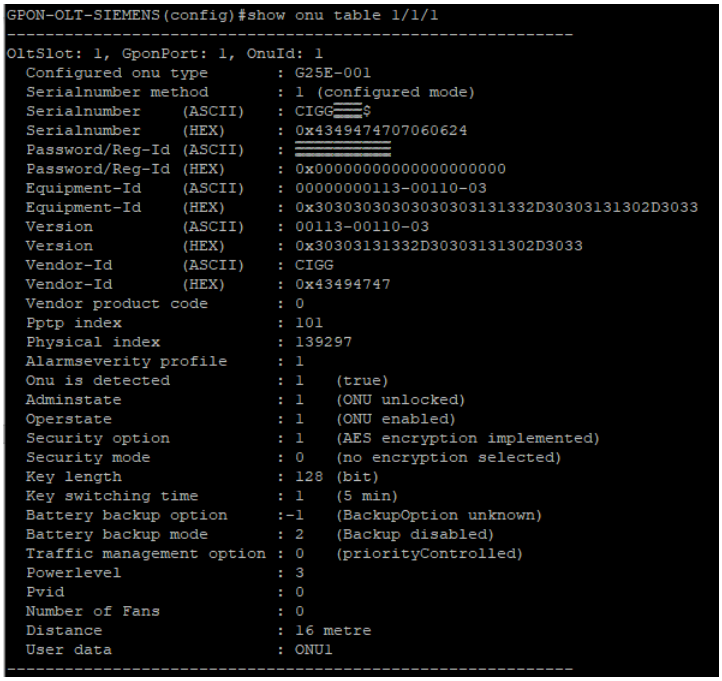
Příkaz pro zobrazení ONU:

GPON-OLT-SIEMENS(config)show onu table 1/1/1

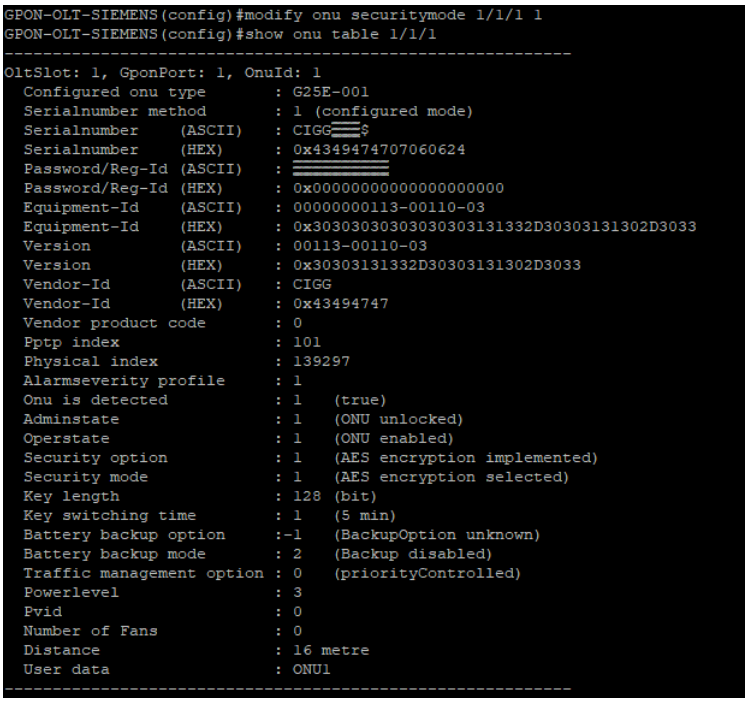
Příkaz pro zapnutí šifrování

GPON-OLT-SIEMENS(config)modify onu securitymode 1/1/1 1

poslední hodnota udává jestli je šifrování zapnuto - 0 pro vypnuto, 1 pro zapnuto :



Obr. 4.17: Výpis nastavení ONU s vypnutým šifrováním komunikace



Obr. 4.18: Nastavení šifrování komunikace

5 Výsledky měření

5.1 Vložení děliče - útlum

Měřením bylo zjišťeno, že nejmenší hodnota útlumu, která vznikne při realizaci útoku se bude pohybovat okolo 0,3 dB. Je důležité zmínit, že tato hodnota velmi závisí na kvalitě veškerých komponent a jejich čistotě. V zájmu útočníka by mělo být použití co nejčistších a nejkvalitnějších spojek SC/FC potažmo konektorů, aby byl vložený útlum co nejmenší. Při nevyčištění konektorů byl útlum v případě děliče 99:1 až trojnásobný. Dále je důležité zmínit, že při výrobě děličů došlo k přehození barev konektorů a hodnoty tak vyšly obráceně, ale správně. K jediným výrazným odchylkám došlo při měření metodou OTDR u děliče 99:1.

5.2 Vložení děliče - čas

Toto měření jasně ukázalo rozdíl mezi časem potřebným pro obnovu komunikace při vložení děliče u point-to-point sítí a pasivních sítí. Samotné vložení zpravidla nezabere více něž 7 sekund, při použití kvalitních konektorů méně než 4 sekundy. U pasivních sítí, konkrétně GPON je třeba počítat s časem potřebným pro vyjednaní časových oken, výměnu klíču atd., který se pohyboval v rozmezí 6 až 41 sekund v extrémních případech. Zpravidla však dosahoval 10 až 25 sekund.

5.3 Makroohyb

V rámci měření bylo zjištěno, jakých hodnot útlumu dosahuje vytvořený ohyb vlákna s jednotlivými poloměry. Z měření vyplývá, že pro vlákna typu G.625 je kritická hranice 14 mm, kdy dochází k strmému nárůstu útlumu, lze tvrdit, že vzestup hodnot nabírá exponenciální růst do doby než dojde k přelomení vlákna, ke kterému došlo u poloměru ohybu 7 mm. Při měření byly veškeré komponenty propojeny konektory SC pro maximální konstantnost mezi oběma scénáři měření.

5.4 Zpětný odraz

Při tomto měření byly stanoveny hodnoty zpětného odrazu u jednotlivých typů běžně používáných konektorů, konkrétně typu SC. Byl zřetelně naměřen a stanoven rozdíl mezi plochou (UPC) a zkosenou (APC) ferulí, který u zapojených konektorů činil 16,65 dB a u nezapojených 14,14 dB.

5.5 Přeslechy vlnových multiplexů

Měření zaměřené na přeslechy vlných multiplexů prokázalo výskyt přeslechů jak u DWDM, tak i u CWDM MUXů. U DWDM MUXu je přeslech zjistitelný na 2 sousedních kanálech s hodnotami okolo 47 dB v případě přímého souseda a 77 dB u 2 kanály vzdálených sousedů. Dále bylo prokázáno, že vztah mezi vstupním výkonem a hodnotou přeslechu je lineární a přímo úměrný. U CWDM MUXu byly zjištěny přeslechy mezi vstupními kanály s hodnotami okolo 65 dB.

5.6 Přeslechy optomechanického přepínače

Optomechanické spínače se pyšní velmi dobrou izolací mezi kanály a malým vloženým útlumem, což bylo ověřeno. Vložený útlum dosahoval hodnot maximálně 1 dB, spíše méně. Hodnota přeslechů byla menší než 70 dBm. Jedinou zjištěnou vadou bylo prohození spínacích pinů - pro přímý prostup měly dle inspection sheetu být použity piny 1 a 5 a pro křížený piny 6 a 10. V případě tohoto konkrétního kusu to však bylo přesně naopak, tedy piny 6 a 10 pro přímý a 1 a 5 pro křížený, na funkčnost zařízení to ale nemělo vliv.

Závěr

Cílem bakalářské práce bylo provedení analýzy možnosti úniku dat z aktivních a pasivních prvků optických vláknových infrastruktur včetně návrhu a ověření vybraných metod. Praktická část byla věnována měření časů a útlumu u vložených optických děličů, měření přeslechů, zpětných odrazů a útlumu makroohybů. Následně došlo k analýze rizik u jednotlivých měření s návrhem minimalizace rizik. Z měření vyplynulo, jak jsou jednotlivé scénáře aplikovatelné a potenciálně nebezpečné. Lze říci, že veškeré útoky cílící na nezašifrovanou komunikaci nelze opomenout a jejich minimalizaci by měla být věnována zvláště velká pozornost. Velmi důležitým závěrem je, že při návrhu a realizaci optických sítí by mělo být dodržováno několik základních pravidel. Jmenovitě: užití kvalitních komponent, šifrování celé komunikace, minimalizace přístupu cizích lidí k infrastruktuře, snaha o co nejnižší vložený útlum trasy a správná implementace NMS. Při dodržení těchto základních pravidel dojde k relativně velké minimalizaci nejběžněji vznikajících rizik, která byla popsána, proměřena a zanalyzována v rámci této bakalářské práce.

Literatura

[1] *K*EISER, Gerd. OPTICAL FIBER COMMUNICATIONS. 4. vydání. New York: McGraw-Hill, 2011, 654 s. ISBN 978-0-07-338071-1

[2] *F*ILKA, Miloslav. Optické přenosy informací pro integrovanou výuku VUT a VŠB-TUO [online]. 2014. Dostupné z: http://optolab.utko.feec.vutbr.cz/wp-content/uploads/SKRIPTA_14-Optick%C3%A9-p%C5%99enosy-informac%C3%A1-pro-integrovanou-v%C3%BDuku.pdf.

[3] *B*UBNÍK, Lukáš, Jíří KAJBL a Petr MAZUCH. Optoelektrotechnika [online]. Code Creator, 2014. ISBN 978-80-88058-20-5. Dostupné také z: https://publi.cz/download/publication/185?online=1.

[4] *H*OLOMEČEK, Petr a Martin HÁJEK. CHROMATICKÁ DISPERZE JEDNOVIDOVÝCH OPTICKÝCH VLÁKEN A JEJÍ MĚŘENÍ [online]. Dostupné také z: https://docplayer.cz/10698556-Chromaticka-disperze-jednovidovych-optickych-vlaken-a-jeji-mereni.html.

[5] *K*YSELÁK, Martin. Disperzní vlivy optických vláken na multiplexní přenosy [online]. Brno, 2008. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace?zp_id=16660. Dizertační práce. Vysoké učení technické v Brně.

[6] *Z*ÁČEK, Martin. Nelineární charakter optického prostředí [online]. Brno, 2008. Dostupné také z: https://dspace.vutbr.cz/handle/11012/9896. Bakalářská práce. Vysoké učení technické v Brně.

[7] *W*hat is telecom optical wavelength bands ? [online]. FiberLabs Incorporated. Dostupné také z: https://www.fiberlabs.com/glossary/about-optical-communication-band/.

[8] *F*ILKA, Miloslav. Optoelektronika pro telekomunikace a informatiku. Brno: Centa, 2009, 369 s. ISBN 978-80-86785-14-1.

[9] *O*ptical Fiber [online]. The Fibre Optic Association, 2015. Dostupné z: https://www.thefoa.org/tech/ref/basic/fiber.html

[10] *N*omenclature For Optical Fibers And Cross Reference To International Standards [online]. The Fibre Optic Association, rok neznámý. Dostupné z: https://www.thefoa.org/tech/smf.htm

[11] *G*IRARD, Andre. FTTx PON Technology and Testing. Quebec: EXFO, 2005. ISBN 1-55342-006-3.

[12] ALWAYN, Vivek. Fiber-Optic Technologies: Fiber-Optic Cable Termination [online]. Cisco Press, 2004. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=170740&seqNum=8

[13] MLEJNEK, Zbyněk. Optické zesilovače. Brno, 2008. Dostupné také z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=8652. Bakalářská práce. Vysoké učení technické v Brně.

[14] MARIA, Furdek a Skorin-Kapov NINA. Physical-Layer Attacks in Transparent Optical Networks [online]. 2012. Dostupné z: https://www.intechopen.com/books/optical-communications-systems/physical-layer-attacks-in-transparent-optical-networks

[15] CALVIN SI, Y. a Yale CHENG. Optical Multiplexer/Demultiplexer. WDM Technologies [online]. Elsevier, 2003, 2003, , 39-78 . ISBN 9780122252624. Dostupné z: doi:10.1016/B978-012225262-4/50005-2

[16] Measuring Reflectance or Return Loss [online]. The Fiber Optic Assiciation, 2018, 2012. Dostupné z: https://www.thefoa.org/tech/ref/testing/test/reflectance.html

[17] EXFO Electro-Optical Engineering Inc, FTTx PON Guide: Testing Passive Optical Network, 2nd edition, Quebec 2004, ISBN-1-55342-002-0.

[18] ZAFAR IQBAL, M, Habib FATHALLAH a Nezih BELHADJ. Optical Fiber Tapping: Methods and Precautions [online]. 2011, , 164-168. Dostupné z: doi:10.1109/HONET.2011.6149809

[19] VONDRUŠKA, Pavel. Crypto-World [online]. 9. 2007. ISSN 1801-2140. Dostupné také z: http://crypto-world.info/casop9/crypto07_07.pdf

[20] DRAKULIC, S., M. TORNATORE a G. VERTICALE. Degradation attacks on Passive Optical Networks. In: Optical Network Design and Modeling (ONDM), 2012[online].Dostupné z: http://ieeexplore.ieee.org/document/6210184/

[21] THOMAS, Stephen a David WAGNER. Insecurity in ATM-based passive optical networks [online]. 2002. Dostupné z: https://ieeexplore.ieee.org/document/997353

[22] SIMONÍK, Jan. Bezpečnostní rizika v pasivních optických sítích [online]. Brno, 2018. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/110108. Bakalářská práce. Vysoké učení technické v Brně.

[23] *A*nalýza a řízení rizik BOZP. Identifikace, hodnocení a management ve firmách a jiných organizacích [online]. BOZP.cz. Dostupné také z: https://www.dokumentacebozp.cz/aktuality/analyza-rizik-bozp-rizeni-hodnoceni-identifikace-management/

Seznam symbolů, veličin a zkratek

WAN	Wide area network
MAN	Metropolitan area network
LAN	Local area network
dB	Decibel
MUX	Multiplexer
DEMUX	Demultiplexer
NDSF	Non dispersion shifted fibre
ORL	Optical return loss
PC	Physical contact
UPC	Ultra physical contact
SPC	Super physical contact
APC	Angled physical contact
SFP	Small form-factor pluggable transciever
FTB	Fused bionic taper
PLC	Planar Lightwave circuit
EDFA	Erbium-doped fiber amplifier
WDM	Wavelenght-division multiplexing
WWDM	wide wavelenght-division multiplexing
CWDM	coarse wavelenght-division multiplexing
DWDM	Dense wavelenght-division multiplexing
AWG	Arrayed waveguide grating
FBG	Fibre bragg grating
OAN	Optical acces network
AON	Active optical network

PON	Pasive optical network
OLT	Optical link termination
ONT	Optical network termination
ONU	Optical network unit
OTDR	Optical time-domain reflectometer
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
APON	Asynchronous transfer mode pasive optical network
BPON	Broadband pasive optical network
GPON	Gigabit pasive optical network
XG-PON	10 gigabit pasive optical network
AES	Advanced encryption standart
NMS	Network management system