VULNERBILITY OF GPON NETWORK ELEMENTS

Jan Chlapek
Master Degree Programme (2nd), FEEC BUT
E-mail: xchlap02@stud.feec.vutbr.cz

Supervised by: Tomas Horvath
E-mail: horvath@feec.vutbr.cz

Abstract: Passive optical network (PON) is a promising access network technology used in modern telecommunications. Due to their passive nature PONs are potentially vulnerable against a number of security threats. This paper is focused on testing the resilience of a GPON (Gigabit PON) network against a DoS (Denial of Service) attack, conducted with a CW (Continuous Wave) laser plugged into the optical splitter. The goal was to cause signal interference on the feeder fiber to prevent communication between the OLT (Optical Line Termination) and ONUs (Optical Network Unit).

Keywords: DoS, Security, GPON, PON, Passive Optical Network

1 ÚVOD

Aktuální trendy moderní technologické doby vyžadují výrazný růst komunikační infrastruktury na poli rychlejších přístupových sítí. Výrazným krokem kupředu je rozšíření přístupových sítí PON (Pasivní optické sítě), u nichž je optické vlákno distribuováno co nejblíže ke koncovým zákazníkům tzv. FTTH (Fiber To The Home), a to pomocí zcela pasivní distribuční sítě [1]. V České republice se ovšem lze nejčastěji setkat pouze s nasazením FTTC (Fiber To The Curb) a FTTB (Fiber To The Building). K finální distribuci konektivity k zákazníkovi pak většinou slouží původní metalické rozvody.

V této práci byla testována zranitelnost plně funkční GPON sítě od společnosti Huawei. Test byl zaměřen na zarušení komunikace mezi koncovými prvky sítě pomocí CW laseru (S Kontinuální vlnou) typu DFB (S rozloženou zpětnou vazbou) s chlazením TEC (Termoelektrickým chlazením).

2 GPON

GPON byl standardizovaný společností ITU-T (International Telecommunication Union) v roce 2003. Výrazně vylepšil vlastnosti svých předchůdců, a to především v použití nové rámcové struktury GEM (GPON Encapsulation Method). Díky této struktuře je možné zajistit přenos velkého množství datových struktur např. Ethernet, hlasové služby, digitální video aj., a proto je též nazývaná jako „Full-service“ služba [1].

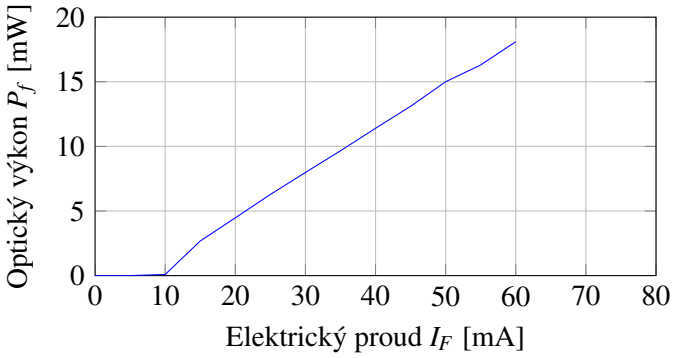
2.1 ZRANITELNOSTI V PON

Díky svým pasivním vlastnostem jsou PON náchylné vůči řadě útoků. U aktivních prvků, především pak u ONU (Optická koncová jednotka), patří mezi největší hrozby bezpečnostní díry ve firmwarech a lehce vyhledatelné servisní přihlašovací údaje, jenž mohou útočníkovi posloužit k plnému přístupu do zařízení. Dalším bezpečnostním rizikem je pasivní rozbočovač, jenž je v PON použit k rozdělení signálu mezi ONU podle daného dělícího poměru. Volný port v rozbočovači může být např. využit k připojení modifikované ONU za účelem odposlechu komunikace nebo k připojení CW laseru za účelem aktivního rušení komunikace. Před rozbočovač je také teoreticky možné umístit modifikovanou OLT jednotku, jenž by v síti sloužila k vykonávání MITM (Man in the Middle) útokům [2].

3 POUŽITÝ LASER

K zarušení signálu byla použita laserová dioda FLD7F4CZ typu DFB, pracující na vlnové délce 1310 nm [5]. Tento typ laseru je vhodný pro vysílání na jedné vlnové délce se spektrální šířkou okolo 1 nm. Naladění na konkrétní vlnovou délku probíhá již během výroby úpravou rozestupů mezi odrazy ve vnitřní struktuře laseru. Laser byl rovněž teplotně stabilizován pomocí TEC, čímž bylo docíleno optimální teploty 25°C dle katalogu výrobce [4]. Laserová dioda je v provedení tzv. motýlku a k jejímu připojení byla použita ovládací platforma CLD1015 od společnosti ThorLabs. Ovládání výstupního výkonu laseru bylo provedeno nastavením elektrického proudu procházejícího diodou I_F.

Před započetím měření byl optický výkon laseru nejdříve změřen na měřiči optického výkonu. Aby nedošlo k poškození měřiče, byl optický výkon měřen s použitím útlumového článku o hodnotě 20 dB. Rozsah I_F byl dále změřen jen do hodnoty 60 mA, zatímco maximální hodnota I_F je dle katalogu 80 mA. To mohlo do vykreslené závislosti na Obr. 1 zanést malou nepřesnost kvůli možným nedokonalostem vzniklých v přechodech mezi konektory, možnou degradací článku a chybějícím hodnotám v rozsahu 60–80 mA.



Obrázek 1: Závislost optického výkonu na elektrickém proudu diodou

Změřená křivka závislosti optického výkonu na elektrickém proudu na Obr. 1 nicméně byla porovnána s referenční křivkou z katalogu [5] a na základě porovnání se shodují. Naměřené hodnoty optického výkonu v rozsahu I_F 0–60 mA jsou v Tab. 1. K přepočtu optického výkonu v jednotkách dBm na jednotky v mW byl použit následující vzorec:

$$P_f = P = 10^{\frac{x}{10}},$$

kde x je hodnota optického výkonu v jednotkách dBm.

4 TESTOVACÍ SÍŤ

K provedení testovaní byla použita fakultní GPON síť od společnosti Huawei. Jako OLT (Optické linkové zakončení) byla použita univerzální OLT platforma Huawei MA5683T, jenž nabízí možnost připojení až šesti karet GPON, XGPON (10G-GPON) nebo EPON (Ethernet PON). V rámci sítě GPON byla použita její nejvyšší specifikovaná útlumová třída C+, jejíž parametry jsou vystiženy v Tab.2.

V testu byla pro OLT použita základní konfigurace, jenž obsahovala jen nejnutnější nastavení a registrované koncové jednotky pro dosažení funkční PON sítě. ODN (Optickou distribuční síť) tvořilo optické vlákno o délce 20 km, jenž bylo následně zapojeno do pasivního rozbočovače. Pro testovací účely této práce byly k dispozici pasivní rozbočovače o dělících poměrech 1:2, 1:4, 1:8 a 1:16. V síti byly zapojeny 3 koncové jednotky. Kompletní schéma zapojení je na Obr. 2

Tabulka 1: Naměřené hodnoty optického výkonu v závislosti na proudu I_F

Proud I_F [mA]	Optický výkon [dBm]	Optický výkon P_f [mW]
5	-22,69	0,00538
10	-0,51	0,889
15	4,28	2,68
20	6,5	4,47
25	7,98	6,28
30	9,02	7,98
35	9,85	9,66
40	10,57	11,4
45	11,16	13,1
50	11,8	15,1
55	12,26	16,8
60	12,58	18,1

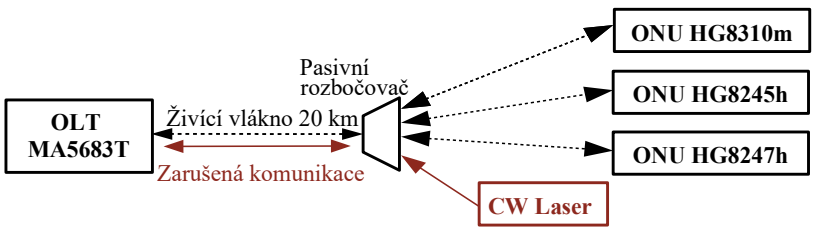
Tabulka 2: Přenosové parametry útlumové třídy C+ [3]

Přenosové parametry optické třídy C+	Sestupný směr	Vzestupný směr
Vlnová délka	1490 nm	1310 nm
Přenosová rychlost	2,488 Gbit/s	1,24 Gbit/s
Minimální vysílací výkon	3 dBm	0,5 dBm
Maximální vysílací výkon	7 dBm	5 dBm
Maximální citlivost přijímače	−32 dBm	−30 dBm
Dosah	20 km	20 km

4.1 Metodika testování

Po ověření referenčních hodnot byl laser připojen společně s ONU do pasivního rozbočovače. V případě dělícího poměru 1:2 byly připojené ONU měněny postupně, zatímco u vyšších dělících poměrů byly připojeny všechna ONU současně.

Jak bylo vyobrazeno na Obr. 2, cílem měření bylo zarušení živícího vlákna, tj. vlákno mezi OLT a pasivním rozbočovačem. Úspěšným zarušením vlnové délky 1310 nm, by došlo k desynchronizaci OLT a ONU a ztrátě připojení ONU k PON síti. Nastavení I_F probíhalo krokově po 5 mA a po zjištění přibližné oblasti výpadku byla výsledná hodnota zjištěna s přesností na desetiny.



Obrázek 2: Schéma zapojení sítě testovací sítě GPON

4.2 VÝSLEDKY

Měření probíhalo na třech modelech ONU od společnosti Huawei. Konkrétní modely jsou vyobrazeny na Obr. 2. Výsledky měření se pro všechny modely odlišovaly minimálně, a proto se v Tab. 3 nacházejí výsledky pouze pro nejvyšší model, a sice model HG8247h.

Tabulka 3: Výsledky pro měření u ONU HG8247h

Dělící poměr [–]	Proud I_F [mA]	Přibližný optický výkon P_f [mW]
1:2	26,6	∼6,5
1:4	43,4	∼12
1:8	75,7	∼19,5

Z výsledků je patrné, že ačkoliv byl použit výkonný CW laser, nebylo možné úspěšně zarušit dělící poměry nad 1:8, kde již laser vyzařoval svůj téměř maximální výkon.

Přesnost výsledků může být zkreslena absencí spektrální analýza CW laseru a ONU za účelem zjištění možného odstupu od pilotní vlnové délky 1310 nm. Dále hodnoty P_f v Tab. 3 nelze považovat za směrodatné, protože přesné hodnoty optického výkonu v závislosti na proudu I_F nebyly změřeny.

Přesto lze z měření vyvodit závěr, že byť PON nedisponují mechanismem na obranu vůči této konkrétní formě útoku, lze samotnou finanční nákladnost v kombinaci s potřebou fyzického přístupu k prvkům PON sítě považovat jako dostatečnou ochranou.

5 ZÁVĚR

Cílem práce bylo realizovat DoS útok na plně funkční testovací GPON síť. Útok byl proveden pomocí výkonného CW laseru typu DFB s chlazením TEC. Úspěšně byla zarušena komunikace pro dělící poměry 1:2, 1:4 a 1:8. K úspěšnosti útoku pro vyšší dělící poměry by bylo zapotřebí vyššího optického výkonu. Na základě výsledků lze konstatovat, že leč je komunikaci v PON pomocí CW laseru možné narušit, vyžaduje tento útok přístup k velmi drahým přístrojům, jmenovitě laserům, případně optickým zesilovačům. Dále by útočník musel získat fyzický přístup k pasivnímu rozbočovači nebo ONU dané PON sítě, aby mohl laser do PON připojit.

REFERENCE

[1] KEISER, Gerd *FTTX concepts and applications*. Hoboken, N.J.: IEEE, 2006. ISBN 978-0-471-70420-1.

[2] HORVATH, Tomas, Lukas MALINA a Petr MUNSTER. On security in gigabit passive optical networks. *2015 International Workshop on Fiber Optics in Access Network (FOAN)* [online]. IEEE, 2015, 51-55 [cit. 2018-11-15]. DOI: 10.1109/FOAN.2015.7320479. ISBN 978-1-4673-7625-9. Dostupné z: http://ieeexplore.ieee.org/document/7320479/

[3] Key Differences Between GPON SFP Class B+ and C+. [Online]. [cit.2018-12-10]. Dostupné z URL: http://gponsolution.com/key-differences-gpon-sfp-class-b-c.html.

[4] Distributed Feedback Lasers. [Online]. [cit.2018-12-10]. Dostupné z URL: https://www.rp-photonics.com/distributed-feedback-lasers.html.

[5] Futjisu 1,310nm MQW-DFB CATV Laser FLD3F7CZ. [Online]. [cit.2018-12-10]. Dostupné z URL: https://datasheet.live/FLD3F7CZ-datasheet.html.