Securing Passive Optical Networks Against Signal Injection Attacks

Harald Rohde, Dominic A. Schupke

Siemens Networks
Otto-Hahn-Ring 6, D-81730 Munich, Germany
Corresponding author: Harald.Rohde@siemens.com

Abstract. Passive optical access networks are susceptible to intended attacks and unintended failures. This paper discusses intrusion by user-side signal-injection resulting in reduced network accessibility and it proposes possible countermeasures. The central function is that an intruding signal can be switched off when it is present.

1. Introduction

Any access network is subject to various intrusions, caused by intended attacks or by unintended failures (employed here analogously to “attacks”). Such attacks can target security items, e.g., information reaches a specific port to which it was not intended, or attacks may concern network accessibility, i.e., the possibility for a single user or a failing terminal to degrade (or even disable) the access network for other connected users. This paper discusses the latter case resulting in degradation or denial of service by signal injection in passive optical access networks. We also suggest countermeasures.

Shared-resources enable us to divide the expenditures of some of the network infrastructure (e.g., the medium) by the number of possible users. The throughput for a single user should not be significantly affected, if only a small fraction of the users at a given time access the resources (statistical multiplexing).

The following list presents some examples for shared-medium networks: Ethernet before the introduction of switches (the name “Ether” refers to the old perception of an ubiquitous medium), all wireless networks, cable modem networks, and within fiber optics Passive Optical Networks (PONs). Shared-resources, however, always raise security issues that have been sufficiently solved for the above network types (e.g., by “switched Ethernet”), except for PONs.

To the best of the authors’ knowledge, the only paper addressing the issue is [1]. The system proposed in [1], however, uses optical fuses that have to be replaced after an attack. Our proposal allows for automatic switching-back to regular state once the attacking signal has been removed. We focus on the critical case of direct injection [2] of continuous signals, however, extension to sporadic signals appears realizable by sophisticated detection functions.

2. Modern passive optical networks

Figure 1 depicts a next-generation passive optical network. One single Optical Line Termination (OLT) handles a number of subscriber units (Optical Network Units, ONUs) on a split-fiber infrastructure. The optical splitter site is at best completely passive. A set of different architectures for this topic are currently under discussion [3-4]. However, apart from pure WDM-PONs, all future PONs have a high splitting-factor in common.

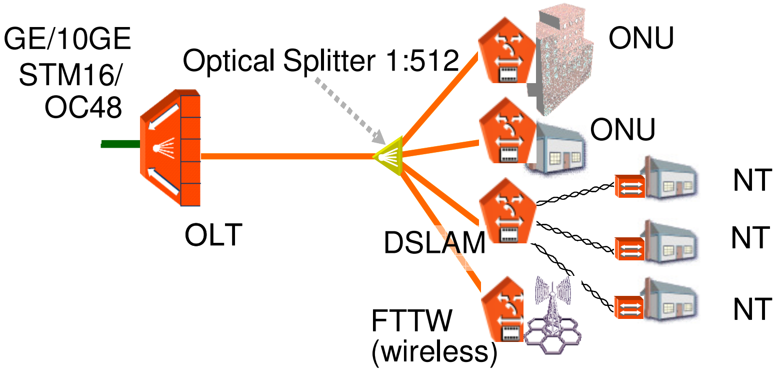

Fig. 1. Typical layout of a next generation passive optical network (PON).

As also depicted in Figure 1, a single OLT serves a number of different user-types. Possible users are private users, small/medium enterprises, wireless stations by Fiber To The Wireless (FTTW), and (outdoor) Digital Subscriber Line Access Multiplexers (DSLAMs) which feed a number of DSL users at the Network Terminations (NTs).

The larger the splitting factor becomes, the higher the danger of intended or unintended network disturbances will be. Because of the shared nature of the upstream data channel (upstream is here defined to be the direction from the ONU to the OLT), a single light source sending permanently or -even worse- casually light with the matching wavelength can stop the operation of the whole PON. While the downstream direction is optically unaffected, the lack of acknowledgment data packets from the single ONUs will immediately stop the operation of the PON.

Sending the light source can be done easily, including hacking into the ONU or using simple hardware. As enterprise users or wireless network operators attached to the ONU would refrain from relying on a network, which a single user could shut down, countermeasures have to be taken.

Today, a single PON has 16 to 32 users per fiber and because of this relatively small number a homogenous group of users (e.g., private-users groups, business-users groups) can be connected. Increasing split factors up to 512 or even higher makes homogenous groups increasingly difficult or even impossible, underlining importance of countermeasures against attacks.

3. Countermeasure against permanent signal injection

For the operator it is obviously interesting to identify the attacking port and to disconnect the attacker from the network. Applying a manual process for this can involve long PON outage durations, since the duration includes sending maintenance personnel to the OLT and checking ports one after another until the attacking port is found. Therefore we propose an automatic process for fast and administratively simpler reaction.

Figure 2 shows a generic architecture allowing to disconnect individual users by controlled optical switches at the splitter. These switches can also serve for other purposes such as for testing toward the ONU.

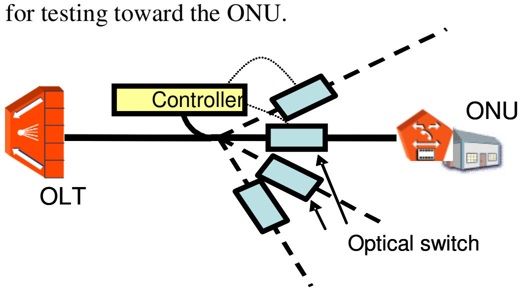

Fig. 2. : Architecture to disconnect attackers.

In the attack-case of sending a permanent signal from some ONU, the controller can firstly detect that such a continuous signal is sent (e.g., by detecting from a tap). Secondly, it identifies the port by briefly disconnecting the users, invoking the switches. This disconnection time should be very short, but still high enough to allow detection (e.g., ~5 ms). Once the attacking port is identified, i.e., when during a switch-off the permanent signal disappears, the corresponding port can be switched off and maintenance personnel can react on the malfunction at the ONU. The important point is that during this process the other users remain almost or even completely unaffected.

While active realizations are possible, for pure passive networks, we aim to realize the controller and the switches such that the splitter-site remains passive. For this, the controller can be placed at the active OLT, where it can detect the attacking signal. The attacking user is then associated with the corresponding switch that the controller addresses for disconnection. For switch activation, the controller can send a switching signal downstream from the OLT to the switches, allowing a passive realization of the switches. Hence, the switches are not invoked by a power supply, but by an optical signal filtered from the incoming OLT signal.

For cost-efficient components, we can use CWDM here. As the number of wavelength could then become exhausted, we can mitigate by addressing port groups (hence, a group of switches) over the invocation signal, that then disconnects a group of users. Such a solution compromises between cost and impact of attack.

In Figure 3 we present two potential technologies for the optical switches. In Figure 3a, only the data wavelength and a selected invocation wavelength can pass through

the CWDM filter. Upon sending an invocation wavelength, the successive absorptive dye becomes opaque and thus can switch off the port, otherwise it remains transparent.
In Figure 3b, a part of the signal is tapped off and passed through a CWDM filter for the invocation wavelength. Upon sending the invocation wavelength, the successive photodiode (PD) generates a voltage that applies to the Mach-Zehnder Modulator (MZM) to switch the fiber optically off.

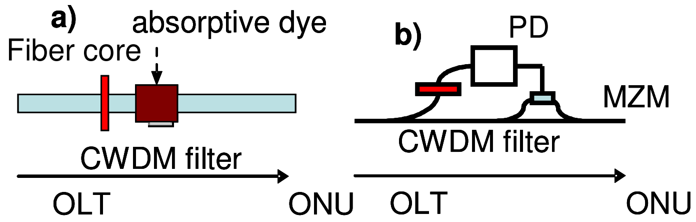

Fig. 3. Possible technologies for the optical switch.

4. Quantitative measure of the benefits

Figure 4 compares the Total Accumulated Outage Time (TAOD) which is defined as the Mean Time to Failure Recovery multiplied by the number of users for the three cases of a standard GPON, an unprotected enhanced PON, and a protected PON. The following assumptions hold: (i) half an hour to get a service technician ready and to get access to the splitter site, (ii) the distances to the splitter are 10 km for the GPON and 90 km for the enhanced PON, (iii) the average driving speed from the central office (where the OLT is based) to the splitter site is 50 km/h and (iv) 5 minutes for each ONU are needed to open the connection, check it and splice it again.
For an enhanced PON with 512 users the TAOD can be over 20 000 hours which can result in a tremendous financial penalty for the network operator. The TAOD for a protected PON with around one second delay until the protection sets in, is less than 10 minutes (512 seconds). The numbers of the example above may be varied, but in any case the TAOD of a protected PON will be 2 to 3 orders of magnitude below the TOAD of an unprotected PON for large user numbers.

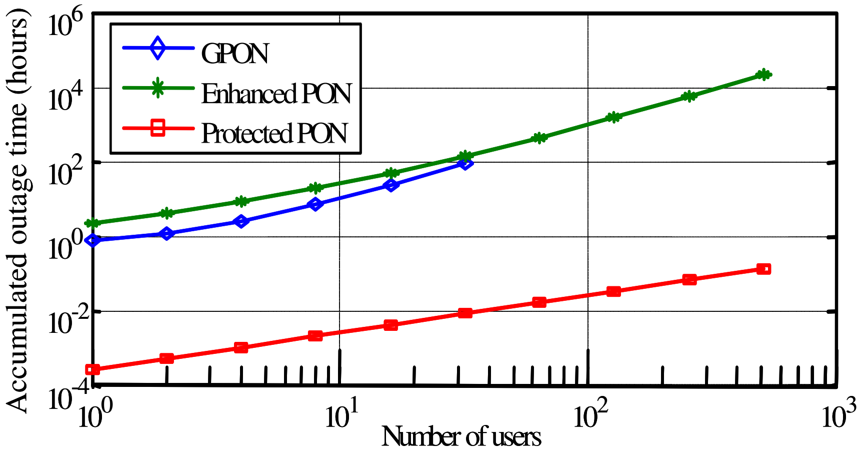

Fig. 4. Accumulated total worst case outage time for GPONs and Enhanced PONs

5. Conclusions

We have tackled a new network security issue which emerges together with the evolution of next-generation passive optical access networks. We discussed the important threat of user-side signal-injection and propose an efficient mechanism countermeasuring against this threat. We expect that in future passive optical networks such protection mechanisms will have to be installed, similarly to existing shared-resources networks.

References

[1] Shing-Wa Wong, Wei-Tao Shaw, Saurav Das, Leonid G. Kazovsky: “Enabling Security Countermeasure and Service Restoration in Passive Optical Networks”, IEEE GLOBECOM, San Francisco, CA, USA, November 27 - December 1, 2006

[2] J-S. Yeom, O.K. Tonguz, "Security and Self-Organization in Transparent Optical Networks", Invited Paper, ACM AccessNets 2006, Athens, Greece, September 2006.

[3] Harald Rohde, ”Modern PON Architectures”, Asia-Pacific Optical Communications Conference (APOC), Shanghai, China, November 6-10, 2005..

[4] Harald Rohde, Sebastian Randel, “Project PIEMAN: A European approach to a symmetrical 10 Gbit/s, 100 km, 32 λ and 512 split PON”, Asia-Pacific Optical Communications Conference (APOC), Gwangju, Korea, September 3-7, 2006.