Security Attacks in Optical Access Networks – Simultaneous Detection and Localization

1: *The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint-Petersburg, Russia*

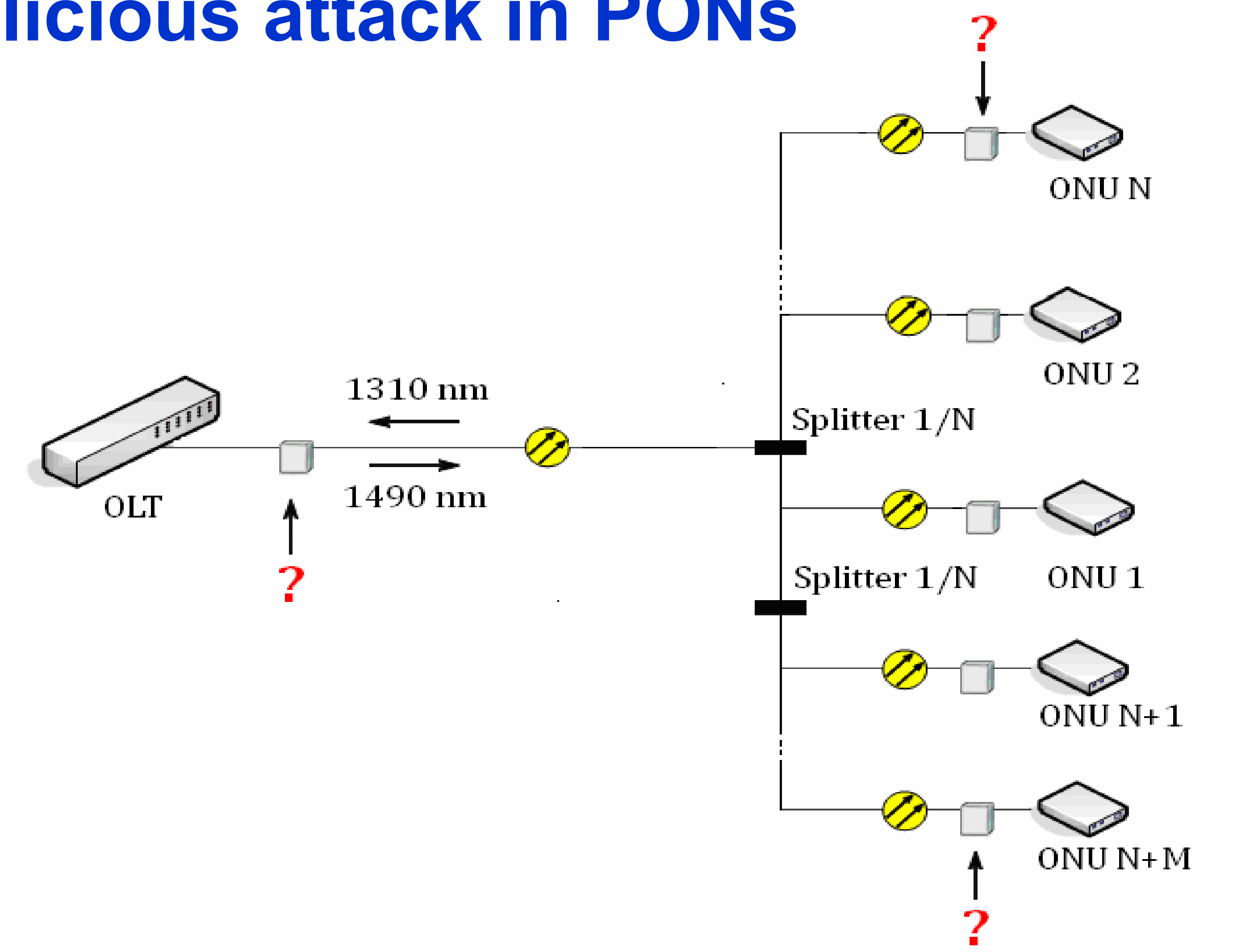
2: *IMAQLIQ Ltd, R&D, Saint-Petersburg, Russia*

3: *DTU Fotonik, Dept. of Photonics Engineering, Technical University of Denmark, Kgs.Lygnby, Denmark*

Outline

- State-of-the-problem
- State-of-the-art
- Macrobends tapping
  - *Macrobend loss investigation*
  - *Simulation model of malicious attack in PONs*
  - *Simulation results*
- Proposed hybrid detection and localization method
- OTDR simulation model
- Concluding remarks

State of the problem: possibility of malicious attack in PONs



IMAQLIQ DTU

Motivation

- No methods or measures have been developed to cope with simple security attacks such as tapping of optical power

Our proposal

- Hybrid monitoring and localization algorithm
- Affected PON branch identification and malicious macrobend localization on an OTDR trace

State-of-the-Art

Non-intrusive methods and techniques

- Rayleigh scattering concentration
- Distributed wave coupling – optical tunneling (1)
- Alternative methods

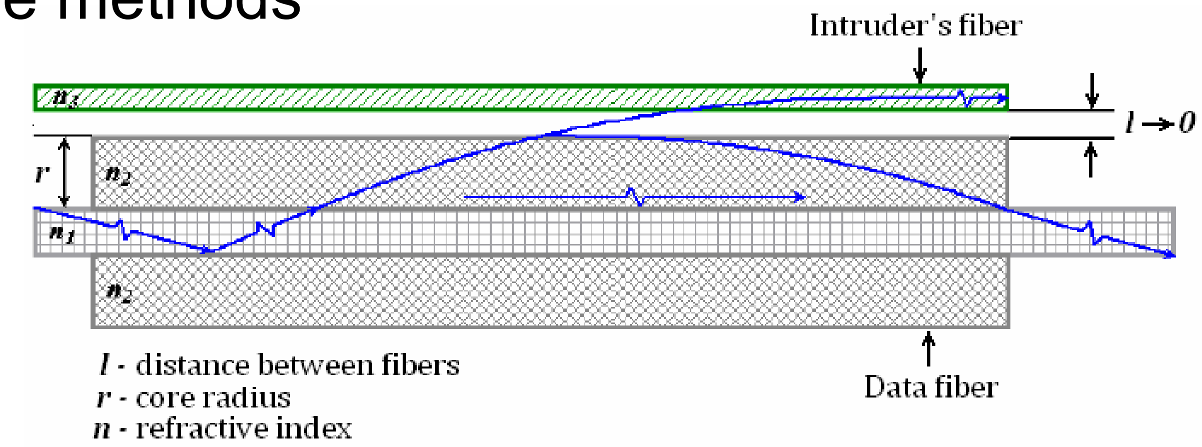


Fig. Optical tunneling

(1) V.V. Grishachev, V.N. Kabashkin, A.D. Frolov, *"Analysis of Channels of Information Leaks in Fiber-Optic Communications: Total Internal Reflection Dysfunctions", Information Counteraction to the Terrorism Threats, Scientific practical magazine, no. 4, 2005, pp. 208-219.*

State-of-the-Art (cont.)

Splicing and coupling (variable)

- Macrobending and clamping
- Coupling
- Acoustical effects
- Temperature perturbations

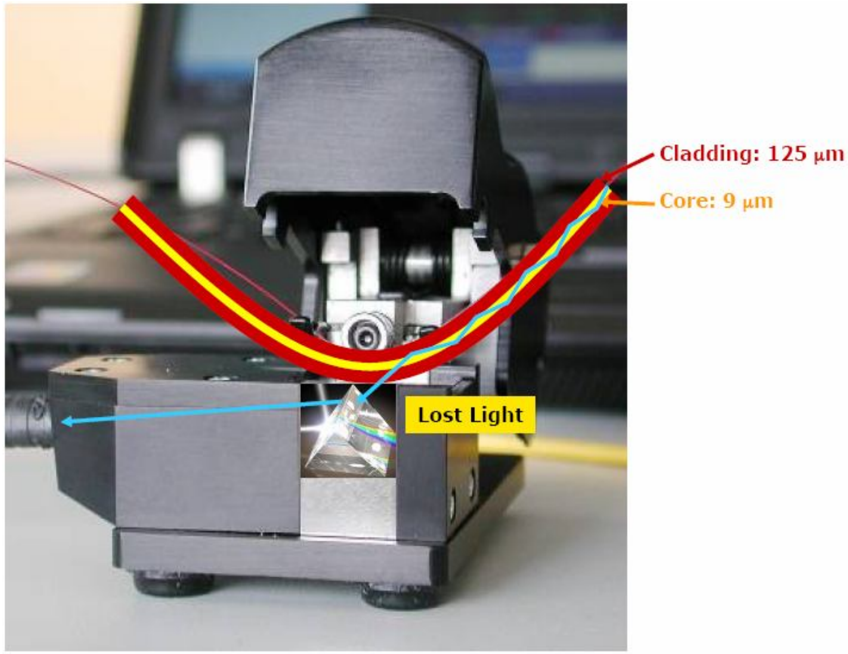
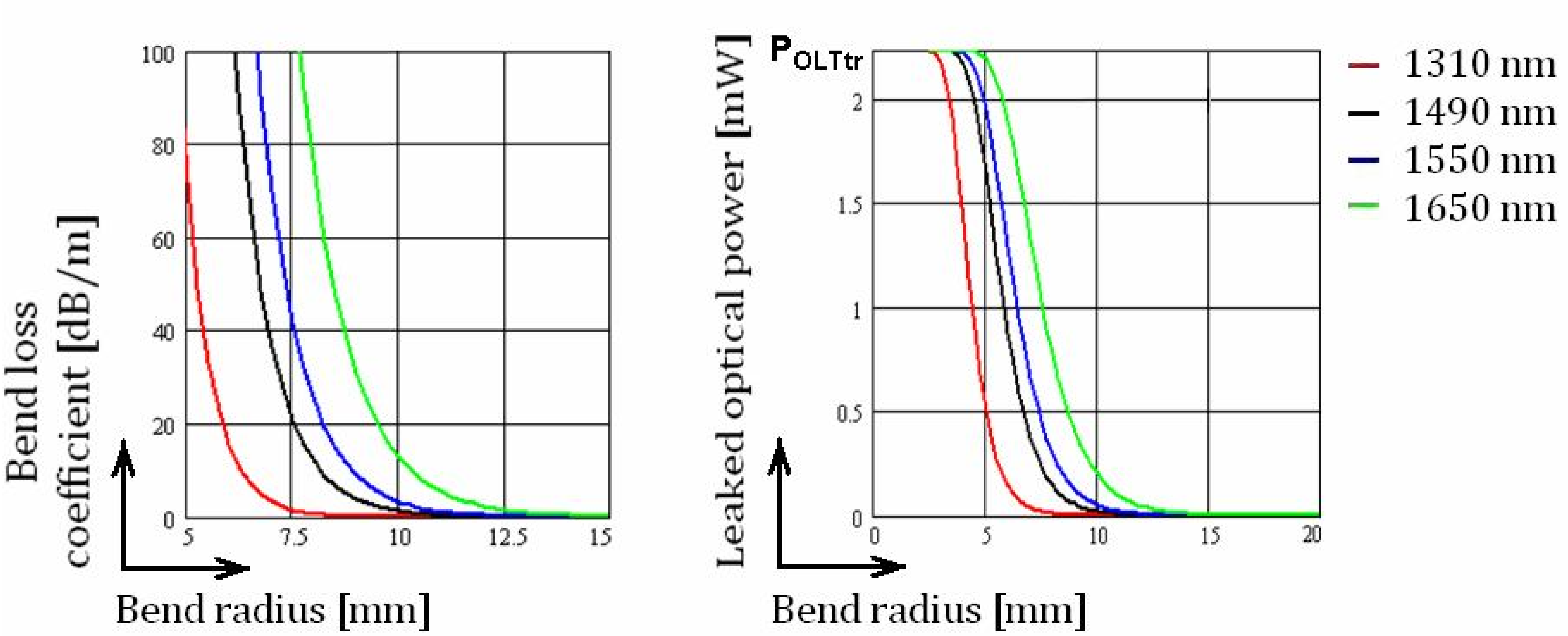


Fig. Clip-on coupling

IMAQLIQ DTU

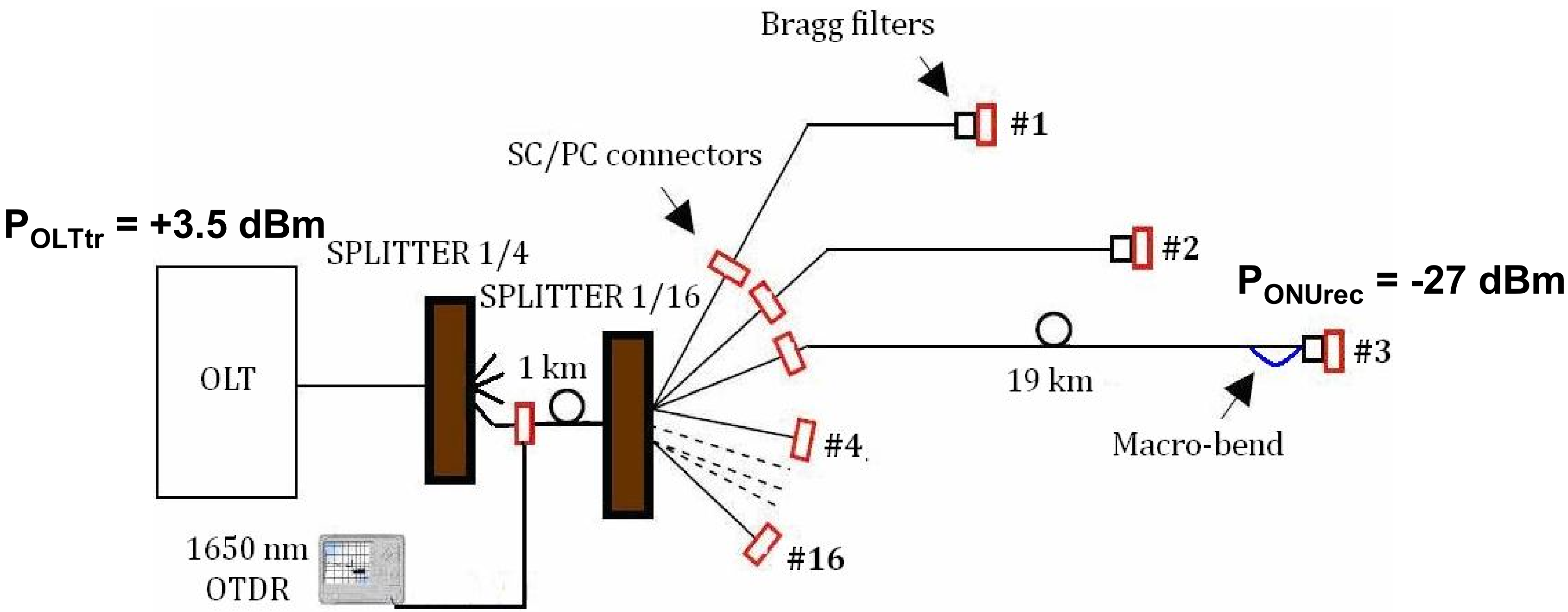
Macrobend loss investigation



- Possibility to extract optical power in PONs by macrobend tapping

IMAQLIQ DTU

Simulation setup



- **OLT**: 2X10 SFF PON Transceiver. High performance 1310 nm burst mode APD receiver and 1490 nm CW mode DFB transmitter
- **ONU**: High performance 1310 nm, 64 nanosecond burst mode F-P transmitter and 1490 nm CW mode P-I-N receiver.

Simulation model of malicious attack in PONs

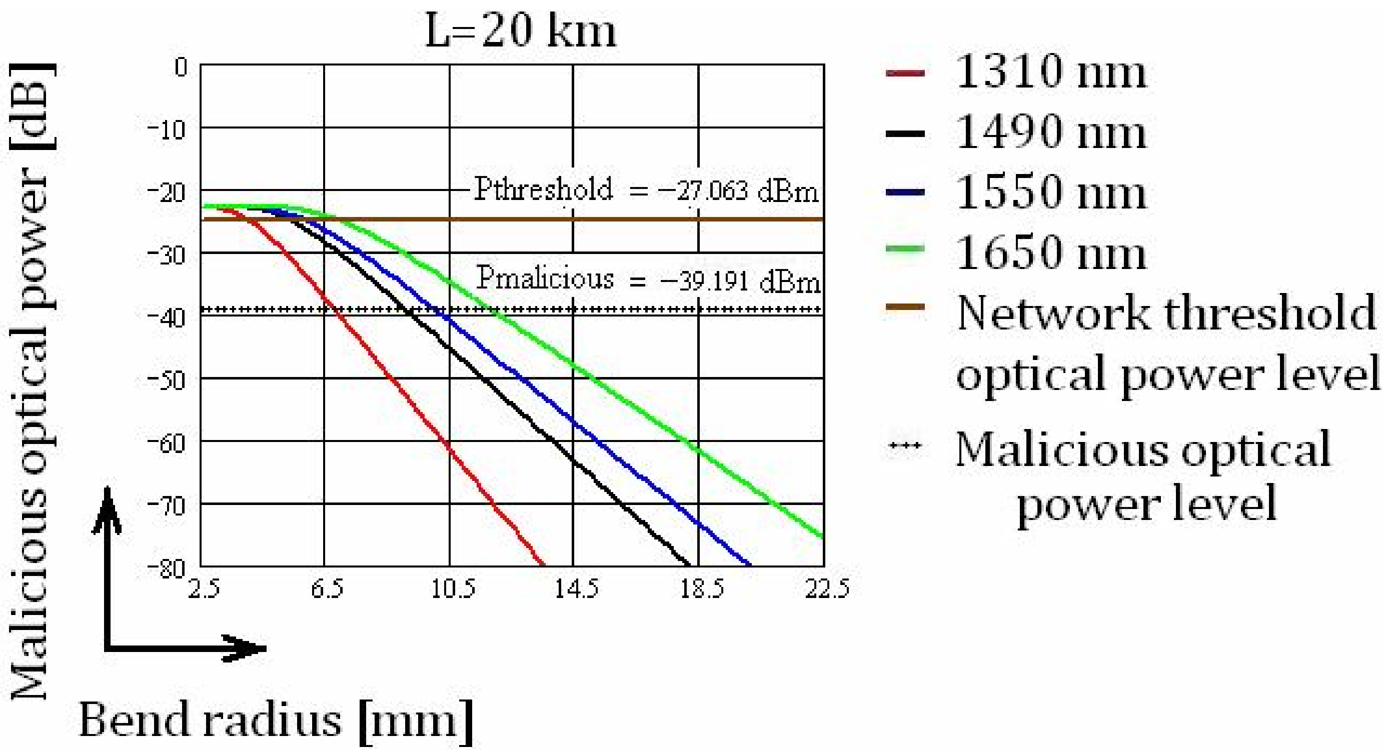
The value of optical power tapped by a half-round macrobend in SMF:

$$P_{malic} = 10 \cdot \lg\left[\eta_{illegal} \cdot P_{OLTtr} \cdot 10^{-\frac{\alpha_0 \cdot l_{malic}}{10}} \cdot 10^{-\frac{\alpha_{fusion}}{10}} \cdot 10^{-\frac{\alpha_{splice}}{10}} \cdot 10^{-\frac{\alpha_{split}}{10}} \left(1 - 10^{-\frac{\alpha_{bend} \cdot \pi \cdot R_{bend}}{10}} \right) \right]$$

$\eta_{illegal}$ – intruder’s photodetector coupling coefficient;
P_{OLTtr} – transmitting optical power from OLT side [mW];
L_{malic} – variable fiber length in situ of potential malicious attack [m];
α_{fusion} – summarized fusion losses [dB];
α_{splice} – summarized splice losses [dB];
α_{split} – summarized planar light circuit (PLC) splitter losses [dB];
R_{bend} – radius of curvature creating by illegal access device [mm].

IMAQLIQ DTU

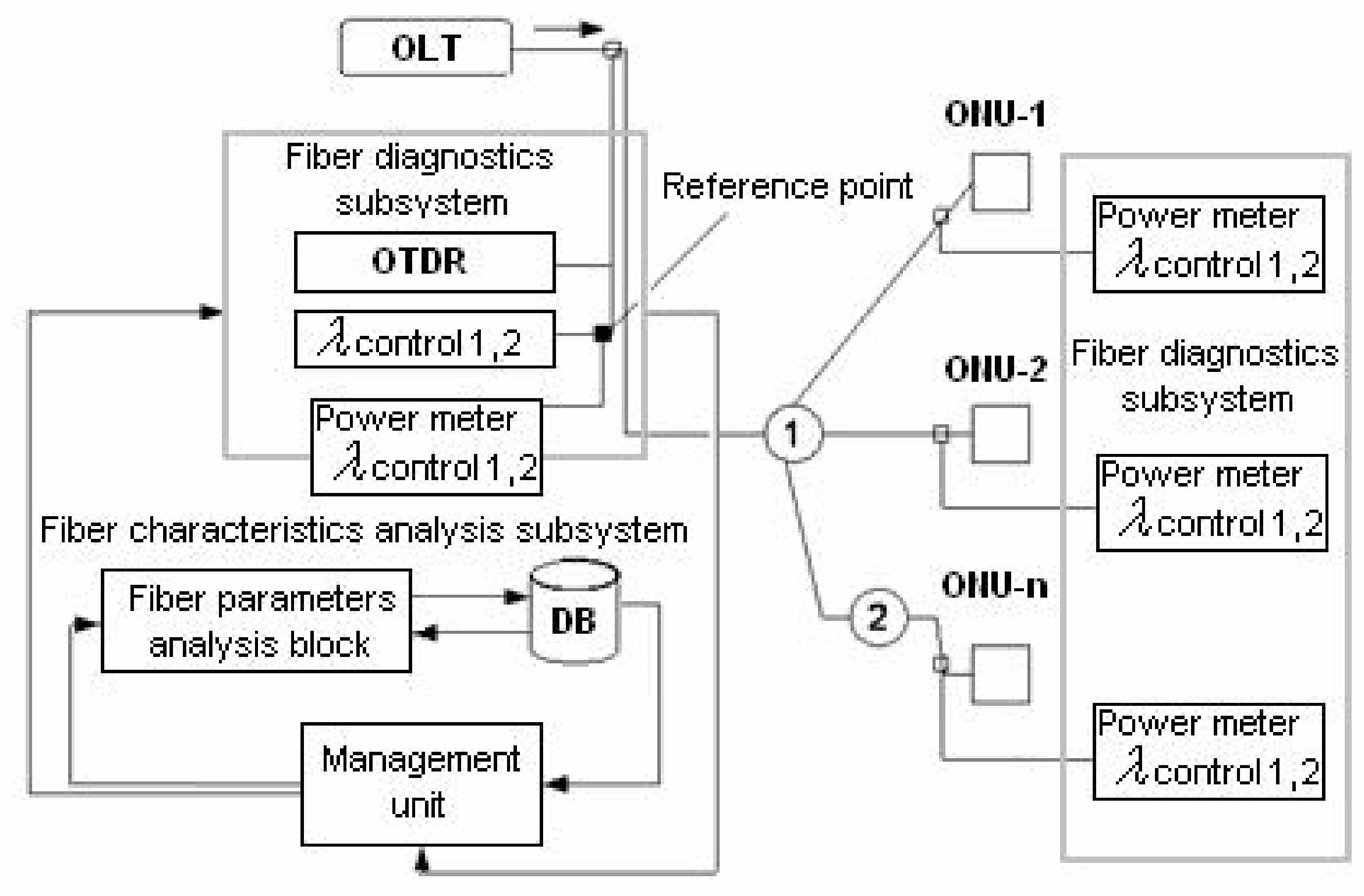
Simulation results



- It's enough to have optical power level equaled to -39.191 dBm
- Management system does not detect it

IMAQLIQ DTU

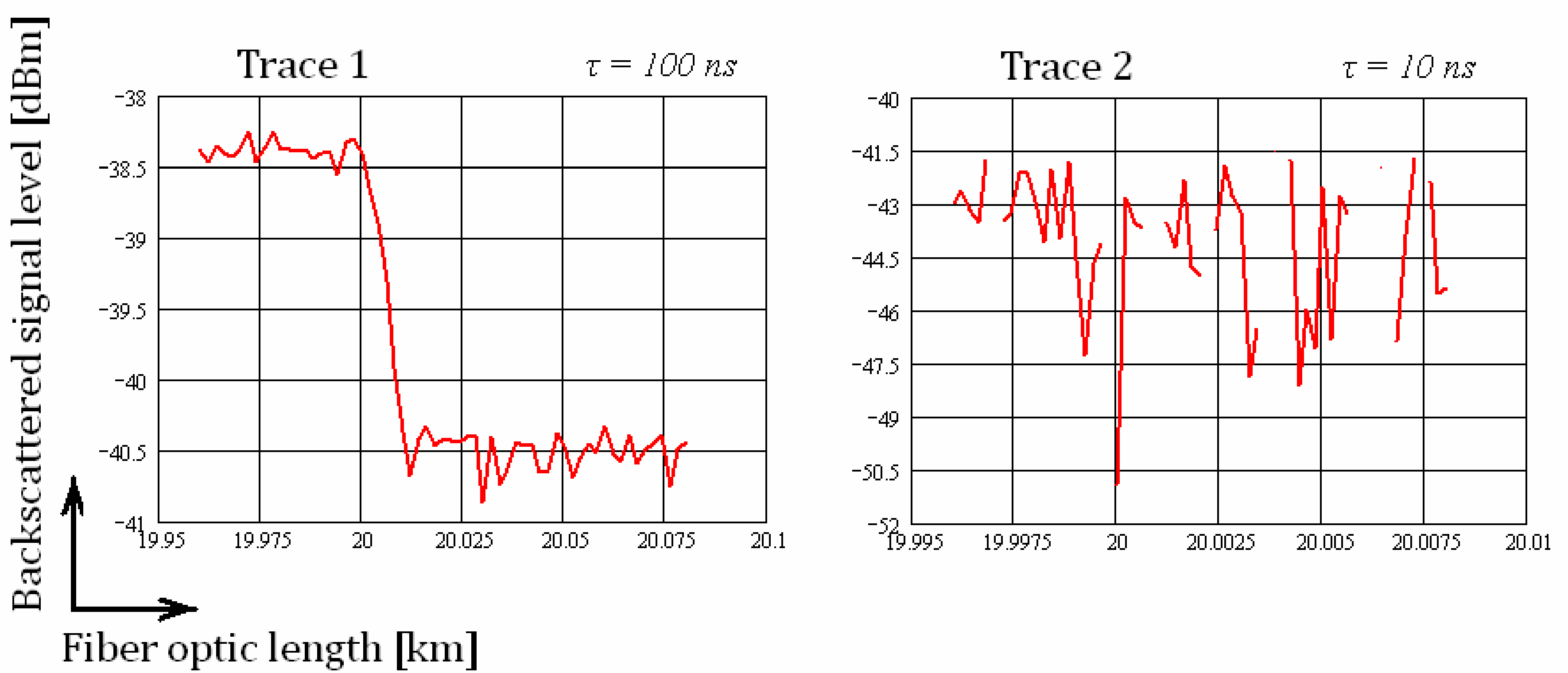
Proposed hybrid detection and localization method



IMAQLIQ DTU

OTDR simulation model

- Optical fiber macrobends correspond to unreflecting heterogeneities



- **Trace 1 shows the acceptable level of macrobend identification**
- **Trace 2 shows a complexity of macrobend identification**

IMAQLIQ DTU

Concluding remarks

- Security break by malicious power tapping is feasible by simple macrobending in common PON standards
- Affected branch identification and attack localization algorithm is proposed
- Potentional deployment by ISP
- Flexibility of implementation for existing PON monitoring systems

Thank you!