SHORT TERM SCIENTIFIC MISSION (STSM) – SCIENTIFIC REPORT

The STSM applicant submits this report for approval to the STSM coordinator

Action number: 15127
STSM title: Experimental demonstration and analysis of physical-layer attacks in optical networks
STSM start and end date: 11/12/2017 to 15/12/2017
Grantee name: Marija Furdek

PURPOSE OF THE STSM

(max.500 words)

Optical networks represent critical infrastructure supporting vital societal services. They are vulnerable to manmade attacks aimed at exploiting inherent vulnerabilities of the optical layer, in order to disrupt services or gain unauthorized access to carried data. Examples of such attacks include insertion of harmful signals to degrade the quality of co-propagating legitimate user signals, or fiber tapping where a part of the optical signal is leaked from the fiber into the hands of an attacker. In order to strengthen the resiliency of optical networks to such attacks, it is important to understand their exact properties and effects to deployed systems.

The purpose of this STSM was to experimentally assess the damaging effects of optical signal insertion and fiber tapping attacks using Telecom Italia's optical testbed facilities. A particular focus is given to examining the performance of coherent receivers in the presence of inserted signals and identifying their vulnerability to attacks, as well as their capability to register anomalous signals. The observed effects and the obtained system performance indicators of a system under different attack scenarios will provide foundation for the subsequent development of attack detection and localization approaches, as well as reactive approaches for network recovery from optical-layer attacks. These activities and outcomes are tightly related to the efforts summarized in RECODIS Working Group 4.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSM

(max.500 words)

The measurements were undertaken on the TIM optical testbed which comprises 185 km of optical fiber connecting Torino with 2 smaller neighboring towns. It is equipped with commercially available coherent transmitters and receivers, Erbium-doped fiber amplifiers and optical time domain reflectometers (OTDR), thus allowing us to examine network conditions very close to real on-field conditions.

The experiments mimicked signal insertion attacks at different frequencies and power levels of the inserted signal. We used a commercially available coherent receiver to detect optical channel performance in the presence of attacks. The analysed parameters included received optical power, optical signal to noise ratio

(OSNR), Q-factor, polarization dependent loss (PDL), chromatic dispersion (CD), differential group delay (DGD), and pre- and post-FEC bit errors.

Constellation diagrams were also recorded.

Two groups of tests were performed:

1) Insertion of an in-band jamming signal

In this test, we analysed the performance of (i) 200G optical channels using 16QAM modulation, and (ii) 100G with QPSK and 15% and 25% FEC. The nominal central frequency of the optical channel under consideration was 193.1 THz. We used 3 auxiliary optical channels at 200G configurations and 6 channels at 100G in order to approach OSNR limit for each modulation format.

The frequency of the jamming signal was tuned from the central frequency of the optical channel under consideration to the 25 GHz detuning in 5 GHz increments. For each frequency, the power of the jamming signal was tuned in 1 dB steps from -7 dB to -0 dB.

2) Insertion of an out-of-band jamming signal

In this test, we analysed the performance of 200G OCh with 193.1 THz central frequency in the presence of a continuous wave (CW) jamming signal inserted at 193.5148 THz with 0 dB, 3 dB and 6 dB power. The loading channels were switched off to improve OSNR. This test also involved a temporal analysis of jamming signal power variations and their influence to the analysed optical channel.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

(max. 500 words)

For the in-band jamming attacks at 200G 16QAM signal, the obtained results indicated that a typical threshold at which the jamming signal causes uncorrected block errors (UBE) in the analysed signal is around -5 dBm. At -15 GHz detuning, the jamming signal causes errors already at -7 dBm, which may be related to the local oscillator frequency of the coherent receiver. When the jamming signal is strongly detuned, the influence is negligible and the required power level to cause errors is at -3 dBm.

The 100G QPSK signal with 15% FEC has been shown as more robust to attacks. UBE threshold for the coupled jamming signal frequency was around -1 dB, dropping to -2 dB for the jamming signal with 15 GHz detuning. Furthermore, 100G QPSK signal with 25% FEC did not have any UBE up to 0 dBm for all jamming signal frequencies.

While the majority of the approaches from the literature consider in-band jamming attacks where the attacking signal has excessive power, our findings show that jamming can cause damage to higher-order modulation formats already at low power levels, which makes this attack method relatively easy to implement.

The second type of attack, i.e., out-of-band jamming, is more demanding as it requires a high-power laser source, but it can also cause larger scale damage. In these measurements, the results shown that time-resolved performance monitoring correctly reports the degradation.

The recorded constellation diagrams indicate that a jamming signal with correctly set state of polarization may induce different noise levels for the x and y polarization states of the observed signal, which may be a valid pointer of an attack.

FUTURE COLLABORATIONS

(max.500 words)

Based on the results obtained during the STSM, KTH and TIM will prepare a conference submission targeting European Conference on Optical Communications (ECOC), and continue the collaboration towards the development of attack detection approaches based on machine learning approaches applied to the collected data sets. The future collaboration will also include joint preparation of project proposals.