Automated Resilience and Secure Networks Operated on Trusted Equipment for Critical Infrastructures and Enterprises

Achim Autenrieth, Jasper Müller, Sai Kireet Patri, Vignesh Karunakaran(1)

(1) Adtran Networks, aautenrieth@adva.com

Abstract Highly available and secure network connectivity is turning into a critical requirement for the European society. This article presents research highlights of the AI-NET-PROTECT project focusing on network automation and AI-based service provisioning in disaggregated optical networks for digital sovereignty. ©2023 The Author(s)

Introduction

Digitization is advancing rapidly in all areas of today's society. Developments such as smart cities, automated transportation, robotics and Industry 4.0 will have a significant impact on people's lives. As our society is become more and more dependent on the network connectivity, a future-oriented communications infrastructure that is available everywhere, sustainably scalable and secure at all times is the basis for successfully driving forward the digitization of the economy and society. Comprehensive network automation is an indispensable prerequisite for the efficient use of such a network infrastructure. It is also the lever to enable a multitude of new digital services and applications, many of which we cannot even imagine today.

In the Celtic-Next project AI-NET-PROTECT (Providing Resilient and Secure Networks Operating on Trusted Equipment to Critical Infrastructures) advanced concepts, network architectures and methods for automated and secure network operation in critical infrastructures and in the economy are being investigated and developed [1]. The focus is on the protection of sensitive and security-relevant data and a high robustness of the network infrastructure. Automated, resilient and secure networks are as important for critical infrastructures and enterprises as they are for the smart city.

Despite huge progress in the deployment of software-defined network control, and advances in streaming telemetry, network data analytics and application of AI for network automation, there are still many open challenges to justify the enormous resources for data collection, storage, and computation of AI.

This article presents research highlights from the AI-NET-PROTECT project contributing to a comprehensive solution for network automation and service provisioning in disaggregated optical networks. It will present recent advances and applications for AI-based QoT estimation, network planning, and transceiver configuration optimization enabling automated network control and service provisioning.

AI-NET-PROTECT reference architecture

Fig. 1 shows the reference optical network architecture defined in AI-NET-PROTECT, which follows the target architecture defined by the OOPT working group of Telecom Infra Project [2]. The architecture supporting automated resilience and service provisioning is envisioned to cover access/metro/core networks and support numerous technologies from different vendors. For intelligent control and network automation, different control protocols, data models, and subscription modes for telemetry streaming are specified.

Fig. 1: Reference architecture of the project AI-NET-PROTECT [1] for disaggregated optical networks with intelligent telemetry & control, AI-based automation, and secure communication
AI for network automation and service providing in disaggregated optical networks

Artificial intelligence is promising to bring benefits in several key areas such as AI-assisted monitoring and soft failure detection for predictive maintenance, intrusion detection to protect against malicious attacks and eavesdropping, as well as network optimization and service provisioning using automated transceiver configuration.

However, there are several challenges to be addressed:
- Access to data
- Data security/sovereignty
- Trusted/explainable AI
- Supplier independent parameters and interfaces

Network monitoring, streaming telemetry and data analytics

Intelligent network control and automation requires not only the detailed knowledge of the inventory, current configuration and state of the network, but also continuous monitoring and streaming of telemetry data to perform network analytics.

AI-NET-PROTECT defined, developed, and demonstrated a telemetry framework with data sovereignty features that allows different vendors share telemetry data with each other while staying in control of their data [3].

The collected data can be used for various network automation applications, which have been recently published:
- Fault detection [5]
- Network planning and operation [6]
- ML-based enhancements for QoT estimation [7]
- System margin estimation [8, 9]

Conclusions

This paper summarizes key research highlights from the AI-NET-PROTECT project. A telemetry framework supporting data sovereignty can provide access to telemetry data in multi-operator and multi-vendor scenarios. Streaming telemetry and MLOps pipelines, network data analytics and AI allows to extract insights from telemetry data for informed decision making and network automation. This supports applications such as soft-failure detection and predictive maintenance, QoT and system margin estimation for automated transceiver configuration. These applications form important building blocks for automated service provisioning and resilience. However, AI should not replace or disregard available domain knowledge and heuristics, but should augment it whenever it provides significant benefits.

Acknowledgements

This work has been partially funded in the framework of the CELTIC-NEXT project AI-NET-PROTECT (Project ID C2019/3-4) by the German Federal Ministry of Education and Research (#16KIS1279K).

References