Chair of Network Architectures and Services
School of Computation, Information, and Technology
Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

Optimizing Threshold Signing with Time Sensitive Networking

Motivation

Threshold signing (TS) is a cryptographic method that allows a group of nodes to collaboratively generate a digital signature without any single node having access to the entire private key. The benefits of TS include enhanced security and fault tolerance, as it requires a minimum number of nodes to cooperate in order to produce a valid signature, reducing the risk of key compromise. When TS nodes must communicate over a crowded network, the performance of the signing system may decrease due to increased latency and potential message congestion. This performance degradation is particularly problematic in time-critical scenarios, where delays in obtaining signatures can hinder the timely execution of transactions or operations.

Time Sensitive Networking (TSN) is a set of standards designed to provide deterministic and low-latency communication over Ethernet networks, ensuring that time-sensitive data is transmitted with minimal delay and jitter.

TSN can help when a TS system is "congested" by allowing us to prioritize TS traffic over other less relevant traffic, thereby improving the performance and reliability of the signing process in time-critical scenarios.

Your goal is to optimize TS performance with TSN under various conditions and design an experiment pipeline showing the effectiveness of your solution using the chair's *EnGINE* experimentation framework.

Your Tasks

- Gain a thorough understanding of TS systems, TSN, and the EnGINE framework.

- Develop a method to consistently generate traffic ("load") that disrupts TS node communication.

- Identify strategies to prioritize TS traffic over other types of traffic using TSN.

- Create an experimental setup that allows for reproducible testing of various TSN optimization strategies under different load conditions.

Prerequisites

- A background in cryptography, networking, and distributed systems is highly recommended.

Contact

Filip Rezabek   rezabek@net.in.tum.de
Holger Kinkelin   kinkelin@net.in.tum.de