Work-In-Progress: Safe and Secure Configuration Synthesis for TSN using Constraint Programming

Introduction & Technologies
Our work targets safety-critical real-time systems as found in the automotive, aerospace or industrial domains. Our network technology of choice is Time-Sensitive Networking (TSN):
- Extension to Ethernet to allow real-time scheduling
- Provides clock synchronisation across network (802.1 ASrev)
- Provides deterministic message scheduling (802.1 Qbv)
- Provides support for message redundancy (802.1CB FRER)

To provide authentication we use Timed Efficient Stream Loss-Tolerant Authentication (TESLA):
- Asymmetric authentication
- Multicast
- Resource efficient

Constraints
- TESLA Interval: Maximum value to fulfill requirements.
- Routing: No cycles, Bandwidth not exceeded, Redundant streams don’t overlap
- Scheduling: No Overlap, Dependencies, TESLA security condition, TSN frame isolation, Function-path deadlines

Solution

Synthetic + Automotive Testcases

Results
- Result 1: TESLA overhead is considerable for small messages
- Result 2: Our solution significantly improves schedulability/laxity compared to an ASAP solution
- Result 3: Scalable up to medium sized architectures

Tool available on GitHub: https://github.com/nreusch/TSNConf

Future Work
Compare with heuristic solution
Evaluate scalability
Compare with other authentication protocols