


## ORIGINAL RESEARCH

# Dependability-aware routing and scheduling for Time-Sensitive Networking

 Niklas Reusch<sup>1</sup>  | Silviu S. Craciunas<sup>2</sup> | Paul Pop<sup>1</sup>
<sup>1</sup>Technical University of Denmark, Kongens Lyngby, Denmark

<sup>2</sup>TTTech Computertechnik AG, Vienna, Austria

## Correspondence

Niklas Reusch, Technical University of Denmark, Kongens Lyngby, Denmark.

 Email: [nikre@dtu.dk](mailto:nikre@dtu.dk)

## Abstract

Time-Sensitive Networking (TSN) extends IEEE 802.1 Ethernet for safety-critical and real-time applications in several areas, for example, automotive, aerospace or industrial automation. However, many of these systems also have stringent security requirements, and security attacks may impair safety. Given a TSN-based distributed architecture, a set of applications with tasks and messages as well as a set of security and redundancy requirements, the authors are interested to synthesise a system configuration such that the real-time, safety and security requirements are upheld. The Timed Efficient Stream Loss-Tolerant Authentication (TESLA) low-resource multicast authentication protocol is used to guarantee the security requirements and redundant disjunct message routes to tolerate link failures. The authors consider that tasks are dispatched using a static cyclic schedule table and that the messages use the time-sensitive traffic class in TSN, which relies on schedule tables (called Gate Control Lists, GCLs) in the network switches. A configuration consists of the schedule tables for tasks as well as the disjoint routes and GCLs for messages. A Constraint Programming-based formulation, which can be used to find an optimal solution with respect to the cost function, is proposed. Additionally, a Simulated Annealing-based metaheuristic, which can find good solution for large test cases, is proposed. The authors evaluate both approaches on several test cases.

## KEYWORDS

authentication, constraint programming, redundancy, security, simulated annealing, TESLA, TSN

## 1 | INTRODUCTION

Many modern safety-critical real-time systems are implemented on distributed architectures. They integrate various software functions with different security and safety requirements over the same deterministic communication network. For example, the network in a modern vehicle has to integrate high-bandwidth video and LIDAR data for Advanced Driver Assistance Systems (ADAS) functions with the highly critical but low bandwidth traffic of, for example, the powertrain functions, but also with the best-effort messages of the low-criticality diagnostic services [1]. Figure 1 presents an example of an ADAS network architecture with redundant routes.

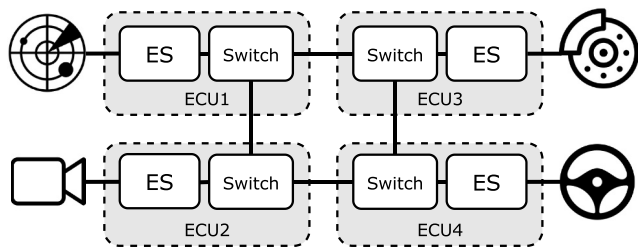
Time-Sensitive Networking (TSN) [2], which is becoming the standard for communication in several application areas, for

example, automotive to industrial control, is comprised of a set of amendments and additions to the IEEE 802.1 standard, equipping Ethernet with the capabilities to handle real-time mixed-criticality traffic with high bandwidth. A TSN network consists of several end-systems that run mixed-criticality applications interconnected via network switches and physical links. Available traffic types are Time-Triggered (TT) traffic for real-time applications, Audio-Video Bridging (AVB) for communication that requires less stringent bounded latency guarantees, and Best-Effort (BE) traffic for non-critical traffic [3].

We assume that safety-critical applications are scheduled using static cyclic scheduling and use the TT traffic type with a given *Redundancy Level* (RL) for communication. We consider that the task-level redundancy is addressed using solutions such as replication [4], and we instead focus on the

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

© 2022 The Authors. *IET Cyber-Physical Systems: Theory & Applications* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.



**FIGURE 1** Automotive Time-Sensitive Networking (TSN)-based Cyber-Physical System (CPS) with redundant routes

safety and security of the communication in TSN. The real-time safety requirements of critical traffic in TSN networks are enforced through offline-computed schedule tables, called Gate Control Lists (GCLs), which specify the sending and forwarding times of all critical frames in the network. Scheduling time-sensitive traffic in TSN is non-trivial (and fundamentally different from e.g., TTEthernet) because TSN does not schedule communication at the level of individual frames as is the case in TTEthernet. Instead, the static schedule tables (GCLs) govern the behaviour of entire traffic classes (queues), which may lead to non-deterministic frame transmissions [5].

Since link and connector failures in TSN could result in fatal consequences, the network topology uses redundancy, for example, derived with methods such as Ref. [6]. In TSN, IEEE 802.1CB Frame Replication and Elimination for Reliability (FRER) enables the transmission of duplicate frames over different (disjoint) routes, implementing merging of frames and discarding of duplicates.

Nowadays, modern Cyber-Physical Systems (CPSs) are becoming increasingly more interconnected with the outside world opening new attack vectors [7, 8] that may also compromise safety. Therefore, the security aspects should be equally important to the safety aspects. Timed Efficient Stream Loss-Tolerant Authentication (TESLA) [9] has been investigated as a low-resource authentication protocol for several networks, such as FlexRay and TTEthernet [10] networks. However, adding security mechanisms such as TESLA after the scheduling stage is often not possible without breaking real-time constraints, for example, on end-to-end latency, and degrading the performance of the system [10]. Thus, we consider TESLA and the overhead and constraints it imposes as part of our configuration synthesis problem formulation.

## 1.1 | Related work

Scheduling for TSN networks is a well-researched problem. It has been solved for a variety of different traffic type combinations (TT, AVB, BE) and device capabilities using methods such as Integer Linear Programming (ILP), Satisfiability Modulo Theories (SMT) or various metaheuristics such as tabu search [3, 5, 11–17].

Routing has also been extensively researched [18, 19]. The authors in Ref. [20] presented an ILP solution to solve the routing problem for safety-critical AFDX networks. In Ref.

[21] the authors used a tabu search metaheuristic to solve the combined routing and scheduling problem for TT traffic in TTEthernet. In Ref. [22] the authors provide a simple set of constraints to solve a general multicast routing problem using constraint programming, which Ref. [6] builds on that to solve a combined topology and route synthesis problem. In Ref. [23], the authors use a load-balancing heuristic to distribute the bandwidth usage over the network and achieve lower latency for critical traffic.

Multiple authors have also looked at the combined routing and scheduling problem. The authors in Ref. [24, 25] showed that they are able to significantly reduce the latency by solving the combined problem with an ILP formulation. In Ref. [26], the authors presented a heuristic for a more complex application model that allows multicast streams. They were able to solve problems that were infeasible to solve using ILP or separate routing and scheduling.

Recently authors have started to present security- and redundancy-aware problem formulations. The authors in Ref. [10] provided a security-aware scheduling formulation for TTEthernet using TESLA for authentication. In Ref. [27], the authors solve the combined routing and scheduling problem and considered authentication using block ciphers. The authors in Refs. [28, 29], on the other hand, present a routing and scheduling formulation that is redundancy-aware but has no security considerations.

To the best of our knowledge, our work is the first one to provide a formulation that is both security and redundancy-aware.

## 1.2 | Contributions

We address TSN-based distributed safety-critical systems and solve the problem of configuration synthesis such that both safety and security aspects are considered. Determining an optimised configuration means deciding on the schedule tables for tasks as well as the disjoint routes and GCLs for messages. Our contributions are the following:

1. We apply TESLA to TSN networks considering both the timing constraints imposed by TSN and the security constraints imposed by TESLA.
2. We formulate an optimisation problem to determine the following: (i) the redundant routing of all messages; (ii) the schedule of all messages, encapsulated into Ethernet frames, represented by the GCLs in the network devices, and (iii) the schedule of all related tasks on end-systems.
3. We extend our Constraint Programming (CP) formulation from Ref. [30] and propose a new Simulated Annealing (SA)-based metaheuristic to tackle large scale networks that cannot be solved with CP.
4. We evaluate the impact of adding the security from TESLA on the schedulability of applications, and we evaluate the solution quality and scalability of the Constraint Programming (CP) and Simulated Annealing (SA) optimisation approaches

We introduce the fundamental concepts of TSN in Section 2 and of TESLA in Section 3. In Section 4, we present the model of our system, consisting of the architecture of the network and applications running on this architecture. Additionally, we present a threat model and how it is addressed by TESLA with a security model. In Section 5, we formulate the problem we are solving using the established models and present an example. In Sections 6 and 7, we present the two different optimisation approaches, CP and SA. Then, we evaluate these approaches using several test cases in Section 8. Section 9 concludes the paper.

## 2 | TIME-SENSITIVE NETWORKING

Time-Sensitive Networking [2] has arisen out of the need to have more stringent real-time communication capabilities within standard Ethernet networks. Other technologies that offer real-time guarantees for distributed systems are TTEthernet (SAE AS6802 [31, 32]), PROFINET, and EtherCAT [33]. TSN comprises a set of (sub-)standards and amendments for the IEEE 802.1Q standard, introducing several new mechanisms for Ethernet bridges, extensions to the IEEE 802.3 media access control (MAC) layer as well as other standards and protocols (e.g., 802.1ASrev). A survey on research results and standardisation efforts for TSN can be found in Ref. [34].

The fundamental mechanisms that enable deterministic temporal behaviour over Ethernet are, on the one hand, the clock synchronisation protocol defined in IEEE 802.1ASrev [35], which provides a common clock reference with bounded deviation for all nodes in the network, and on the other hand, the timed-gate functionality (IEEE 802.1Qbv [36]) enhancing the transmission selection on egress ports. The timed-gate functionality (IEEE 802.1Qbv [36]) enables the predictable transmission of communication streams according to the predefined times encoded in schedules called Gate-Control Lists (GCL). A stream in TSN definition is a communication carrying a certain payload size from a talker (sender) to one or multiple listeners (receivers), which may or may not have timing requirements. In the case of critical streams, the

communication has a defined period and a maximum allowed end-to-end latency.

Other amendments within TSN (c.f. [2]) provide additional mechanisms that can be used either in conjunction with 802.1Qbv or stand-alone. IEEE 802.1CB [37] enables stream identification, based on, for example, the destination MAC and VLAN-tag fields in the frame as well as frame replication and elimination for redundant transmission. IEEE 802.1Qbu [38] enables preemption modes for mixed-criticality traffic, allowing express frames to preempt lower-priority traffic. IEEE 802.1Qci [39] defines frame metering, filtering, and time-based policing mechanisms on a per-stream basis using the stream identification function defined in 802.1CB.

We detail the Time-Aware Shaper (TAS) mechanism defined in IEEE 802.1Qbv [36] via the simplified representation of a TSN switch in Figure 2. The figure presents a scenario in which communication received on one of the two available ingress ports (A and B) will be routed to an egress port C. The switching fabric will determine, based on internal routing tables and stream properties, to which egress port a frame belonging to the respective stream will be routed (in our logical representation, there is only one egress port). Each port will have a priority filter that determines which of the available eight traffic classes (priorities) of that port the frame will be enqueued in. This selection will be made based on either the PCP field of the 802.1Q VLAN-tag of frames or the *stream gate instance table* of 802.1Qci, which can be used to circumvent traffic class assignment of the PCP code. As opposed to regular 802.1Q bridges, where the transmission selection sends enqueued frames according to their respective priority, in 802.1Qbv bridges, there is a Time-Aware Shaper (TAS), also called timed-gate, associated with each traffic class queue and positioned before the transmission selection algorithm. A timed-gate can be either in an *open (o)* or *closed (C)* state. When the gate is open, traffic from the respected queue is allowed to be transmitted, while a closed gate will not allow the respective queue to be selected for transmission, even if the queue is not empty. The state of the queues is encoded in a local schedule called Gate-Control List (GCL). Each entry defines a time value and a state (o or C) for each of the eight queues. Hence, whenever the local clock reaches the specified

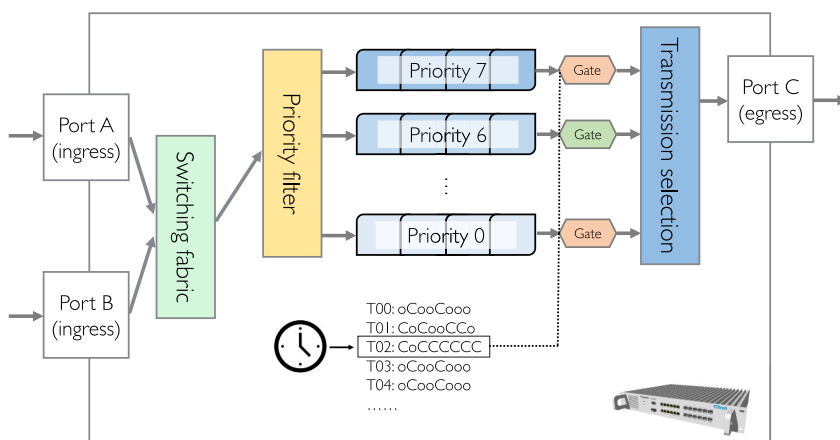


FIGURE 2 Simplified Time-Sensitive Networking (TSN) switch representation

time, the timed-gates will be changed to the respective open or closed state. If multiple non-empty queues are open simultaneously, the transmission selection selects the queue with the highest priority for transmission.

The Time-Aware Shaper functionality of 802.1Qbv, together with the synchronisation protocol defined in 802.1ASrev, enables a global communication schedule that orchestrates the transmission of frames across the network such that real-time constraints (usually end-to-end latencies) are fulfilled. The GCL schedule synthesis problem has been addressed in Ref. [5, 11, 12, 40] for ensuring deterministic communication behaviour for critical streams.

Craciunas et al. [5] define correctness conditions for generating GCL schedules, resulting in a strictly deterministic transmission of frames with 0 jitter. Apart from the technological constraints, for example, only one frame transmitted on a link at a time, the deterministic behaviour over TSN is enforced in Ref. [5] through isolation constraints. Since the TAS determines the temporal behaviour of entire traffic classes and not of individual frames, the queue state always has to be deterministic and hence, Ref. [5] enforces a strict isolation of critical streams by not allowing two critical streams to be enqueued in the same queue at the same time. This condition is called *frame/stream isolation* in Ref. [5]. In Ref. [11], critical streams are allowed to overlap to some degree (determined by a given jitter requirement) in the same queue in the time domain, thus relaxing the strict isolation.

Both approaches enforce that gate states of different scheduled queues are mutually exclusive, that is, only one gate is open at any time, thus preventing the transmission selection from sending frames based on their assigned traffic class's priority. By circumventing the priority mechanism through the TAS, it is ensured that no additional delay is produced through streams of higher priorities, thus enforcing a highly deterministic temporal behaviour.

### 3 | TIMED EFFICIENT STREAM LOSS-TOLERANT AUTHENTICATION

TESLA provides a resource-efficient way to do asymmetric authentication in a multicast setting [9]. It is described in detail in Ref. [9, 41].

We are considering systems where one end-system wants to send a multicast signal to multiple receiver end-systems, for example, periodic sensor data. A message authentication code (MAC), which is appended to each signal, can guarantee authenticity, that is, that the sender is whom he claims to be, and integrity, that is, that the message has not been altered. The MAC is generated and authenticated by a secret key that all end-systems share (i.e., symmetric authentication). The downside of this approach is that if any of the receiving end-systems is compromised, the attacker would be able to masquerade as the sender by knowing the secret key. In a multicast setting, an asymmetric approach, in which the receivers do not have to trust each other, is preferable.

The traditional asymmetric authentication approach is to use asymmetric cryptography with digital signatures (i.e., private and public keys); however, as stated in Ref. [42], the method is computationally intensive and not well suited for systems with limited resources and strict timing constraints.

TESLA, however, uses an approach where the source of asymmetry is a time-delayed key disclosure [9]. While this can be implemented with much less overhead, it requires time synchronisation between the network nodes. For TSN, the time synchronisation is given through the 802.1ASrev protocol.

Figure 3 visualises the TESLA protocol. As described in Ref. [42], when using TESLA, time is divided into fixed intervals of length  $P_{\text{int}}$ . At start-up, a one-way chain of self-authenticating keys  $K_i$  is generated using a hash function  $H$  where  $K_i = H(K_{i+1})$ . Each key is assigned to one interval. The protocol is bootstrapped by creating this chain and securely distributing  $K_0$  to all receivers [10].

Normally in TESLA, as described in Ref. [10], when a sender sends a message  $m$  in the  $i$ th interval, it appends to that message:  $i$ , a keyed-MAC using the key of that interval  $K_i$ , and a previously used key  $K_{i-d}$ . Thus, a key remains secret for  $d$  intervals. When a receiver receives a message  $m$  in the interval  $i$  it cannot yet authenticate it and must wait until a message arrives in the interval  $i + d$ . This message discloses  $K_i$ , which can be used to decrypt the MAC of  $m$  and thus authenticate it. To ensure that  $K_i$  itself is valid, we can use any previously validated key. For example, we can check that  $H(K_i) = K_{i-1}$ ,  $H(H(K_i)) = K_{i-2}$  etc. This makes TESLA also robust to packet loss since any lost keys can be reconstructed from a later key, and any key can always be checked against  $K_0$ .

Due to the deterministic nature of our schedule, we can make some modifications to the basic TESLA protocol without sacrificing security. The first modification is adopted from Ref. [10]. Since bandwidth is scarce, we do not release the key  $K_{i-d}$  with every message/stream. Instead, it will be released once in its own stream with an appropriate redundancy level. The second modification concerns the TESLA parameter  $d$ , the key disclosure delay. This parameter is useful in a non-deterministic setting since the arrival time of a stream is uncertain. A high value for  $d$  means that the corresponding key is released later, making it more likely that a stream can be authenticated, at the cost of increased latency [41]. However, in our case, we know the exact time a stream will be sent and arrived. Thus, we assume that a stream's keyed-MAC will be generated using the key from the interval it *arrives at the last receiver*. We will always release the key  $K_i$  in the interval  $i + 1$ , minimising the key disclosure delay and thus the latency before a stream can be authenticated.

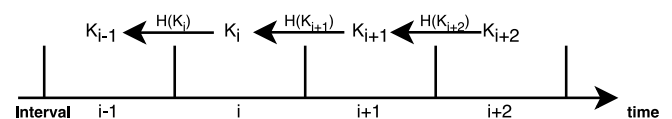


FIGURE 3 TESLA key chain (adapted from [42])

## 4 | SYSTEM MODELS

This section presents the architecture and application models as well as the threat, security, and fault models. Our application model is similar to the one used in related work [10], but we have extended it to consider TSN networks and the optimisation of redundant routing in conjunction with scheduling (Table 1).

### 4.1 | Architecture model

We model our TSN network as a directed graph consisting of a set of nodes  $\mathcal{N}$  and a set of edges  $\mathcal{L}$ . The nodes of the graph are either end-systems (ESs) or switches (SWs):  $\mathcal{N} = \mathcal{ES} \cup \mathcal{SW}$ . The edges  $\mathcal{L}$  of the graph represent the network links.

We assume that all of the nodes in the network are TSN-capable, specifically that they support the standards 802.1ASrev [35] and 802.1Qbv [36]. Thus, we assume the whole network, including the end-systems, to be time-synchronised with a known bounded precision  $\delta$ . All nodes use the time-aware shaper mechanism from 802.1Qbv to control the traffic flow.

Each end-system  $e_i \in \mathcal{ES}$  features a real-time operating system with a periodic table-driven task scheduler. Hash computations, which will be necessary for TESLA operations on that end-system, take  $e_i.H$   $\mu$ s.

A network link between nodes  $n_a \in \mathcal{N}$  and  $n_b \in \mathcal{N}$  is defined as  $l_{a,b} \in \mathcal{L}$ . Since in Ethernet-compliant networks all links are bi-directional and full-duplex, we have that for each  $l_{a,b} \in \mathcal{L}$  there is also  $l_{b,a} \in \mathcal{L}$ . A link  $l_{a,b} \in \mathcal{L}$  is defined by a link speed  $l_{a,b}.s$ .

Figure 4a shows a small example architecture with four end-systems, two switches, and full-duplex links.

### 4.2 | Application model

An application  $\lambda_l \in \Lambda$  is modelled as a directed, acyclic graph consisting of a set of nodes representing tasks  $\Gamma_l$  and a set of edges  $\mathcal{E}_l$  represents a data dependency between tasks.

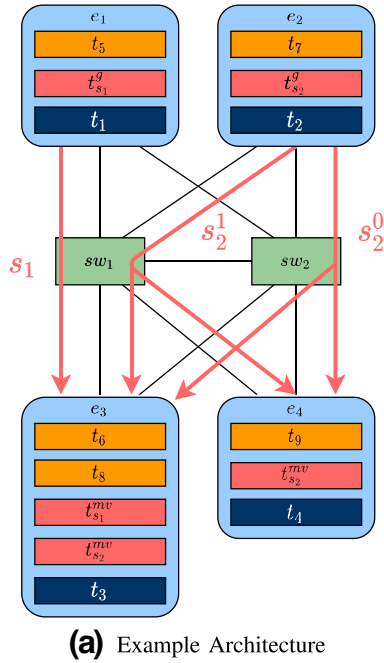
A task is executed on a certain end-system  $t_m.e$ . The worst-case execution time (WCET) of a task is defined by  $t_m.w$   $\mu$ s. A task needs all its incoming streams (incoming edges in the application graph) to arrive before it can be executed. It produces outgoing streams at the end of its execution time. Communication dependencies between tasks that run on the same end-system are usually performed via, for example, shared memory or message queues, where the overhead of reading/writing data is negligible and included in the WCET definition of the respective tasks. Dependencies between tasks on separate end-systems constitute communication requirements and are modelled by streams. A stream in the TSN context is a communication requirement between a sender and one (unicast) or multiple (multicast) receivers. An example application can be seen in Figure 4b. An application is periodic

TABLE 1 Notations

Description	Notation	Unit
Header overhead	OH	Byte
Maximum transmission unit	MTU	Byte
TESLA key size	KS	Byte
TESLA MAC size	MAC	Byte
Hyperperiod	H	$\mu$ s
TSN network graph	$(\mathcal{N}, \mathcal{L})$	
Nodes	$\mathcal{N} = \mathcal{ES} \cup \mathcal{SW}$	
End-system	$e_i \in \mathcal{ES}$	
Hash computation time	$e_i.H$	$\mu$ s
Switch	$sw_j \in \mathcal{SW}$	
Links	$\mathcal{L} \subseteq \mathcal{N} \times \mathcal{N}$	
Network link	$l_{a,b}$	
Link speed	$l_{a,b}.s$	$\mu$ s
Application	$\lambda_l \in \Lambda$	
Tuple	$(\Gamma_l, \mathcal{E}_l)$	
Period	$\lambda_l.T$	$\mu$ s
Communication depth	$\lambda_l.C$	
Tasks	$t_m \in \mathcal{T}$	
Execution end-system	$t_m.e$	
Worst-case execution time	$t_m.w$	$\mu$ s
Period	$t_m.T$	$\mu$ s
Streams	$s_n \in \mathcal{S}$	
Source task	$s_n.t_s$	
Destination tasks	$s_n.T_d$	
Size	$s_n.b$	Byte
Period	$s_n.T$	$\mu$ s
Redundancy level	$s_n.r_l$	
Security level	$s_n.sl$	
MAC generation task	$t_n^g$	
MAC verification task	$t_n^{mv}$	
Security application	$\lambda_l^s \in \Lambda^{\text{sec}}$	
Key release task	$t_m^r$	
Key verification task	$t_m^v$	
Key source end-system	$t_m^v.src$	
Key stream	$s_n^k \in \mathcal{S}_k$	

with a period  $\lambda_l.T$ , which is inherited by all its tasks and streams.

A stream  $s_n$  originates at a source task  $s_n.t_s$  and travels to a set of destination tasks  $s_n.T_d$  (since we consider multicast streams). The stream size  $s_n.b$  is assumed to be



### Application 1 ( $\lambda_1$ ):

$$\lambda_1 \cdot T = 1000 \mu s$$

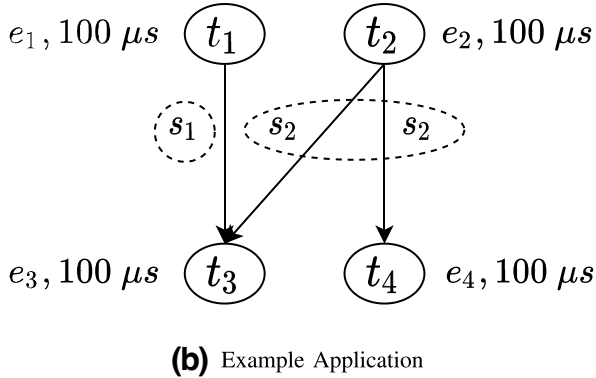


FIGURE 4 Example architecture and application models

smaller than the MTU (maximum transmission unit) defined for the network. Each stream has a redundancy level  $s_n \cdot rl$ , which determines the amount of required disjunct redundant routes for the stream to take. For each of these routes we model a sub-stream:  $s_n^i \in S_{s_n}, 0 \leq i < s_n \cdot rl$ . Hereby  $S_{s_n}$  is a set containing all sub-streams of  $s_n$ . This notation is useful for differentiating the different routes a stream takes through the network and making sure those routes do not overlap. A stream also has a binary security level  $s_n \cdot sl$  which determines if it is authenticated using TESLA ( $sl = 1$ ) or not ( $sl = 0$ ).

We define the hyperperiod  $H$  as the least-common multiple of all application periods:  $H = \text{lcm}(\{\lambda_i \cdot T \mid \lambda_i \in \Lambda\})$ . We define the set  $\mathcal{T}$  to contain all tasks and the set  $\mathcal{S}$  to contain all streams (including redundant copies).

## 4.3 | Fault model

Reliability models discussed in Ref. [6] (e.g., Siemens SN 29500) indicate that the most common type of permanent hardware failures is due to link failures (especially physical connectors) and that ESs and SWs are less likely to fail. These models are complementary to Mean Time to Failure (MTTF) targets established for example, in the automotive domain within the SIL levels of the ISO 26262 certification standard [6]. As mentioned, we assume we know the required redundancy level to protect against permanent link failures. Our disjoint routing can guarantee the transmission of a stream of RL  $n$  despite any  $n - 1$  link failures. For example, for the routing of  $s_2$  with RL 2 in Figure 4a, any 1-link failure would still result in a successful transmission.

## 4.4 | Threat model

We use a similar threat model as Ref. [10] and assume that an attacker is capable of gaining access to some end-systems of our system, for example, through an external gateway or physical access.

We consider that the attackers have the following abilities:

- They know about the network schedule and the content of the streams on the network;
- They can replay streams sent by other ES;
- They can attempt to masquerade as other ES by faking the source address of streams they send;
- They have access to all keys released and received by the ES they control;

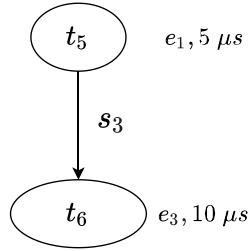
## 4.5 | Security model

We use TESLA to address the threats identified in the previous section, which means that additional security-related models are required. These additional applications, tasks and streams can be automatically generated from a given architecture and application model.

First off, we need to generate, send, and verify a key in each interval for each set of communicating end-systems. We generate a key authentication application  $\lambda_s \in \Lambda^{\text{sec}}$  for each sender end-system, which is modelled similarly to a normal application as a directed acyclic graph. The period  $\lambda_s \cdot T$  is equal to  $P_{\text{int}}$  (see Section 3) and again inherited by tasks and streams. Each of these applications consists of one key release task  $t_m^r$  scheduled on the sending end-system  $e_i$ . Additionally, it consists of key verification tasks  $t_j^v$  on each end-system  $e_j$  that receives a stream from  $e_i$ . The release task sends a multicast key stream  $s_n^k$  to each of those verification tasks. The redundancy level of a key stream  $s_n^k \cdot rl$  is set to the maximum redundancy level of all streams emitted by  $e_i$ . The size of a key stream  $s_n^k \cdot b$  is equal to the key size  $KS$  specified by the TESLA implementation. The security model for our example from Figure 4 can be seen in Figure 5.

**Security Application 1 ( $\lambda_2$ ):**

$$\lambda_2.T = P_{int}$$

**Security Application 2 ( $\lambda_3$ ):**

$$\lambda_3.T = P_{int}$$

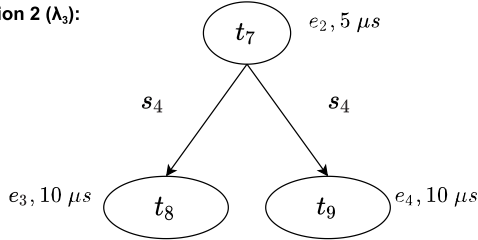


FIGURE 5 Example security model for the applications in Figure 4

For a key verification task,  $t_m^v.src$  is the end-system  $e_i$  whose key this task is verifying. Its execution time is equal to the length of one hash execution on its execution end-system:  $t_m^v.w = (t_m^v.e).H$ . A key release task's execution time is very short, since the key it releases has already been generated during bootstrapping. We model it to be last half the time of a hash execution:  $t_m^r.w = \frac{(t_m^r.e).H}{2}$ .

Secondly, we need to append MACs to all non-key streams with  $s_n.sl = 1$ . Thus, their length increases by the MAC length specified by the TESLA implementation. For each stream  $s_n$ , a MAC generation task  $t_{s_n}^g$  is added to the sender and a MAC validation task  $t_{s_n}^{mv}$  to each receiver. Those tasks take the time of one MAC computation on the processing element to execute.

We define the set  $\mathcal{T}_{kr}^n$  to contain all key release tasks and  $\mathcal{T}_{kv}^n$  to contain all key verification tasks for a given node  $n$ . Furthermore, let  $S_k$  contain all key streams.

Figure 4a shows key release and verification tasks in orange and MAC generation and validation tasks in red.

Figure 5 shows the security applications for our example.

## 5 | PROBLEM FORMULATION

Given a set of applications running on TSN-capable end-systems that are interconnected in a TSN network as described in the architecture, application, and security models in Section 4, we want to determine a system configuration consisting of the following:

- an interval duration  $P_{int}$  for TESLA operations,
- the routing of streams,
- the task schedule, and
- the network schedule as 802.1Qbv Gate-Control Lists (GCLs),

such that

- all deadline requirements of all applications are satisfied.
- the redundancy requirements of all streams and the security conditions of TESLA are fulfilled.
- the overall latency of applications is minimised.

### 5.1 | Motivational example

We illustrate the problem using the architecture and application from Figure 4. We have one application Figure 4b with 4 tasks, 2 streams and a period and deadline of 1000  $\mu$ s. The tasks are mapped to the end-systems as indicated in the figure. Stream  $s_2$  will be multicast. The size of both streams is 50 B. For TESLA's security requirements, that is,  $s_1.sl = s_2.sl = 1$ , we generate two additional security applications (Figure 5).

We have a TSN network with a link speed of 10 Mbit/s and zero propagation delay. Our TESLA implementation uses keys that are 16 B and MACs that are 16 B. A hash computation takes 10  $\mu$ s on every ES.

A solution that does not consider the security and redundancy requirements is shown in Figure 6a. With the TSN stream isolation constraint outlined in Section 2 taken into consideration, the GCLs are equivalent to frame schedules. We depict in Figure 6a the GCLs as a Gantt chart, where the red rectangles show the transmission of streams  $s_1$  and  $s_2$  on network links, and the blue rectangles show the tasks' execution on the respective end-systems. To guarantee deterministic message transmission in TSN, we have to isolate the frames in the time (or space) domain, leading to the delay of  $s_1$  and thus  $t_3$ . We refer the reader to Ref. [5] for an in-depth discussion on the non-determinism problem and isolation solution in TSN.

We are interested in solutions such as the one in Figure 6b, which considers both the redundancy and security requirements. The black dashed line in the figure separates the TESLA key release intervals, where  $P_{int}$  was determined to be 500  $\mu$ s. Streams carrying keys are orange, key generation tasks pink, key verification tasks green, and the MAC generation/validation operations on ESs are shown in red. The routing of the non-key streams can be seen in Figure 4a. Note how the two redundant copies of  $s_2$ ,  $s_2^0$  and  $s_2^1$  use non-overlapping paths.

The delay incurred by the time-delayed release of keys is particularly important: tasks  $t_3$  and  $t_4$  can only be executed after the keys authenticating  $s_1$  and  $s_2$  have arrived in the second interval, and after key verification and MAC validation tasks have been run.

Scheduling problems such as the one addressed in this paper are NP-hard as they can be reduced to the Bin-Packing problem [43] and may be intractable for large input sizes. In the following sections, we will propose a Constraint Programming (CP) formulation to solve the problem optimally for small test cases and a heuristic to solve the problem for large test cases.

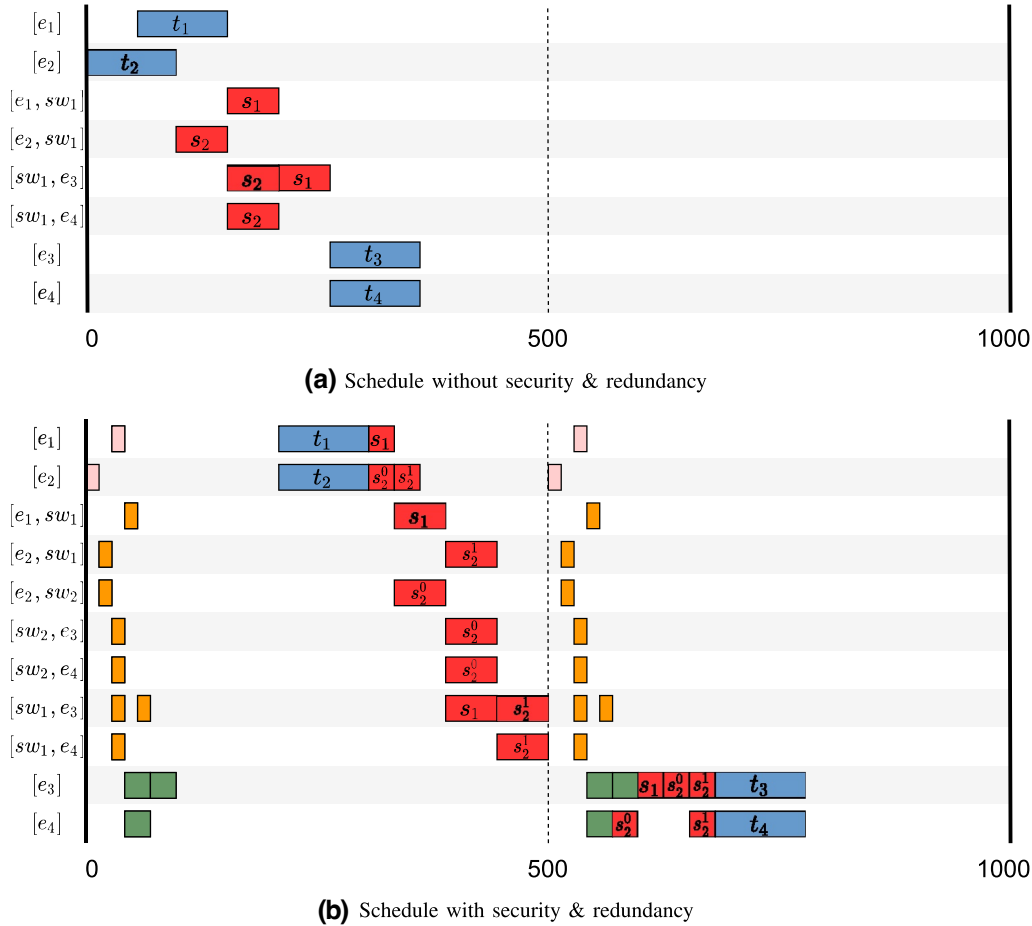


FIGURE 6 Example solution schedules for the models in Figure 4

## 6 | CONSTRAINT PROGRAMMING FORMULATION

Constraint Programming (CP) is a technique to solve combinatorial problems defined using sets of constraints on decision variables. For large scheduling problems, it becomes intractable to use CP due to the exponential increase in the size of the solution space [44]. In order to achieve reasonable runtime performance, we split the problem into three sub-problems which we solve sequentially: (i) finding a route for all streams, (ii) finding  $P_{int}$ , and (iii) finding the network and task schedule.

### 6.1 | Optimising redundant routing

The first step of solving the proposed problem is to find a set of (partially) disjoint routes for each stream, depending on the stream's redundancy level. The constraints in this section are inspired by Ref. [6, 22].

We model the stream routes with an integer matrix  $X$ , where the columns represent streams (including their redundant copies) and rows represent nodes of the network. An entry at the position of a stream  $s_n$  and a node  $n$  in this matrix

referring to a node  $m$ , represents a link from  $m$  to  $n$  on the route of stream  $s_n$ . Alternatively, the entry could be *nil*, in which case  $n$  is not part of the route.

Using the matrix  $X$ , we can construct the route for each stream bottom-up as a tree by starting at the receiver nodes. See Table 2 for the matrix of our example.

To determine the route for each stream  $s_n \in \mathcal{S}$ , for each node  $n \in \mathcal{N}$  we have the following optimisation variables:

- $x(s_n, n)$  represents an entry of our matrix  $X$ . The domain of  $x(s_n, n)$  is defined as follows:  $D(x(s_n, n)) = \{m \in \mathcal{N} | l_{m,n} \in \mathcal{L}\} \cup \{n\} \cup \{nil\}$ . We refer to  $x(s_n, n)$  as the successor of  $n$  on the path to the stream sender node.
- $y(s_n, n)$  represents the length of the path from  $n$  to  $s_n.t_s.e$ , that is, the length of the path from node  $n$  to the sender node of the stream.  $D(y(s_n, n)) = \{i | 0 \leq i \leq |SW| + 1\}$

Furthermore, we define a few helper variables and functions. First off, we define  $\mathcal{S}^d$  as the set of all distinct streams, that is, excluding the redundant copies of streams with the redundancy level (RL) greater than one. Additionally, we define  $\mathcal{S}_{s_d}$  as the set of all redundant copies (including the stream itself) of  $s_d$ . Then we define the following helper function:



**TABLE 2** Matrix X for example from Section 5.1

X	s1	s2_0	s2_1
ES1	ES1	nil	nil
ES2	nil	ES2	ES2
ES3	SW1	SW1	SW2
ES4	nil	SW1	SW2
sSW1	ES1	ES2	nil
SW2	Nil	Nil	ES2

$$xsum(s_d, n, m) = \sum_{s'_d \in S_{s_d}} (x(s'_d, n) == m) \quad (1)$$

This function allows us, for any given  $s_d \in S^d$ , to determine the number of redundant copies (including  $s_d$  itself) that uses the link from  $m$  to  $n$  (nil is counted as zero).

Then we have the following constraint optimisation problem:

$$\text{Minimize : } \sum_{s_n \in S} cost(s_n) \quad (\text{RC1})$$

where

$$cost(s_n) = \sum_{n \in \mathcal{N} \setminus \{s_n.t_s.e\}} (x(s_n, n) \neq nil) \quad (\text{RC2})$$

s.t.

$$x(s_n, n) \neq nil \Rightarrow \gamma(s_n, n) = \gamma(f, x(s_n, n)) + 1, \quad (\text{R1})$$

$$\forall s_n \in S, n \in \mathcal{N} \setminus \{s_n.t_s.e\}$$

$$x(s_n, m) = nil \Leftrightarrow x(s_n, n) \neq m, \quad (\text{R2})$$

$$\forall s_n \in S, n, m \in \mathcal{N}$$

$$x(s_n, n) \neq nil, \quad (\text{R3.1})$$

$$\forall s_n \in S, n \in \{t_r.e | t_r \in s_n.T_d\}$$

$$x(s_n, s_n.t_s.e) = s_n.t_s.e, \quad (\text{R3.2})$$

$$\forall s_n \in S$$

$$x(s_n, n) = nil, \quad (\text{R3.3})$$

$$\forall s_n \in S, n \in \mathcal{E}S \setminus \{t_r.e | t_r \in s_n.T_d\}$$

$$\gamma(s_n, s_n.t_s.e) = 0, \quad (\text{R4})$$

$$\forall s_n \in S$$

$$\sum_{s_d \in S^d} \left( (xsum(s_d, n, m) > 0) \times \frac{s_d.b}{s_d.T} \right) \leq [m, n].s, \quad (\text{R5})$$

$$n, m \in \mathcal{N}$$

$$x(s_n, n) \neq x(s'_n, n), \quad (\text{R6})$$

$$\forall s_n \in S, s'_n \in S_{s_n} \setminus s_n, n \in \mathcal{N} \setminus \{s_n.t_s.e\},$$

Please note that  $==$  and  $!=$  are Boolean expressions that evaluate to 1 if true and to 0 otherwise.

The cost function we are minimising ((RC1), (RC2)) measures the length of the route of each stream.<sup>1</sup>

The constraint (R1) prevents cycles in the route, as defined in Ref. [22]. The constraint (R2) disallows ‘loose ends’, that is, a node that has a successor/predecessor must have a predecessor/successor itself. Please note that we refer to the successor on the path from the receiver to sender, that is, the predecessor on the route. The constraint (R3.1) states that all receivers of a stream have to have a successor. The constraints (R3.2), (R3.3), and (R4) impose that the sender of the stream has itself as the successor, no other end-system has a successor, and the path length is 0 at the sender node, respectively. The constraint (R5) restricts the bandwidth usage of each link to be under 100%. If multiple copies of the same stream use the same link, only one of them is counted as consuming bandwidth since we assume that streams are intelligently split and merged using IEEE 802.1CB. The constraint (R6) forbids the routes of redundant copies of a stream to overlap at any point.

## 6.2 | Optimising $P_{\text{int}}$

To set up the TESLA protocol, we need to choose the parameter  $P_{\text{int}}$ .  $P_{\text{int}}$  is the duration of one key disclosure interval. It has a big influence on the latency of secure streams and thus on the feasibility/quality of the schedule.

When choosing  $P_{\text{int}}$  there is a trade-off between overhead and latency. A small  $P_{\text{int}}$  reduces the latency of secure streams but necessitates more key generation/verification tasks and key streams. Thus, we want to determine the maximum value of  $P_{\text{int}}$  for which the latency is still within all deadline bounds. To this end, we formulate constraints inspired by Ref. [10] for which we then determine the optimal solution. This value is used as a constant in the subsequent optimisation of the schedule.

We introduce a new notation: For each application  $\lambda_l \in \Lambda$  we define  $\lambda_l.C$  to be the communication depth, that is, the length of the longest path in the application graph where only edges with associated secure streams are counted (ES-internal dependencies and non-secure streams are ignored). This gives us a measure of the longest chain of secure communications

<sup>1</sup>For some use cases, fully disjoint routes are not necessary. Refer to Appendix A for an updated formulation for this case.

within the application, which we can use to estimate the amount of necessary TESLA intervals. Then we have the following:

$$\text{Maximize} : P_{int} \quad (\text{P0})$$

s.t.

$$\forall \lambda_l \in \Lambda, \quad P_{int} \cdot (\lambda_l \cdot C + 1) \leq \lambda_l \cdot T \quad (\text{P1})$$

$$H \bmod P_{int} = 0 \quad (\text{P2})$$

$$\begin{aligned} P_{int} \bmod \gcd(\{\lambda_l \cdot T | \lambda_l \in \Lambda\}) &= 0 \quad \text{or} \\ P_{int} * n &= \gcd(\{\lambda_l \cdot T | \lambda_l \in \Lambda\}), \quad n \in \mathbb{N} \end{aligned} \quad (\text{P3})$$

The constraint (P1) guarantees that  $P_{int}$  is small enough to accommodate the authentication of all secure streams for all applications. The communication depth  $\lambda_l \cdot C$  of an application gives a lower bound of how many TESLA intervals are necessary to accommodate all these streams within the period of the application since there have to be  $n + 1$  intervals to accommodate the authentication of  $n$  secure streams.

The purpose of the constraints (P2) and (P3) is to align the TESLA intervals with the schedule. The (P2) makes  $P_{int}$  a divisor of the hyperperiod, while constraint (P3) makes  $P_{int}$  either a multiple or a divisor of the greatest common divisor of all application periods.

### 6.3 | Optimising scheduling

In this step, we want to find a schedule for all tasks and streams that minimises the overall latency of streams while fulfilling all constraints imposed by deadlines, TESLA, and TSN. The routes for each stream and  $P_{int}$  are given by the previous scheduling steps and assumed constant here.

We define the following integer optimisation variables:

- $o_l^s$ : offset of stream  $s$  on link or node  $l$
- $c_l^s$ : transmission duration of stream  $s$  on link or node  $l$
- $a_l^s$ : end-time of stream  $s$  on link or node  $l$
- $\varphi^s$ : index of the earliest interval where stream  $s$  can be authenticated on any receiver
- $o_n^t$ : offset of task  $t$  (on node  $t.e$ )
- $a_n^t$ : end-time of task  $t$  (on node  $t.e$ )

As an example, let us assume a hyperperiod of 1000  $\mu\text{s}$  and a stream  $s$  with a period of 500  $\mu\text{s}$ .  $o_l^s = 100$ ,  $c_l^s = 50$ ,  $a_l^s = 150$  would imply that the stream  $s$  is scheduled on link  $l$  in the following time intervals: (100, 150) and (600, 650).

We also define several helper variables. Let  $\mathcal{E}^s$  be the set containing all receiver end-systems of stream  $s$ :

$$\mathcal{E}^s = \{t.e | t \in s.T_d\}$$

Let  $\mathcal{R}^s$  be the set containing all links on the route of stream  $s$  as well as the sender and receiver nodes:

$$\mathcal{R}^s = \{s.t.s, e\} \cup \mathcal{E}^s \cup \{l_{a,b} | x(s, b) = a, l_{a,b} \in \mathcal{L}\} \quad (2)$$

Using these helper functions we define the following constraint-optimisation problem for the task and network scheduling step:

$$\text{Minimize} : \sum_{\lambda_l \in \Lambda} \text{cost}(\lambda_l) \quad (\text{CS1})$$

where

$$\text{cost}(\lambda_l) = \max(\{a^t | t \in \Gamma_l\}) - \min(\{o^t | t \in \Gamma_l\}) \quad (\text{CS2})$$

s.t.

$$\begin{aligned} \text{cost}(\lambda_l) &\leq \lambda_l \cdot T \\ \forall \lambda_l &\in \Lambda \end{aligned} \quad (\text{S1})$$

$$\begin{aligned} o_l^s &= c_l^s = a_l^s = 0, \\ \forall s \in \mathcal{S}, l_{a,b} \in \mathcal{L}, l_{a,b} &\notin \mathcal{R}^s \end{aligned} \quad (\text{S2.1})$$

$$\begin{aligned} o_n^s &= c_n^s = a_n^s = 0, \\ \forall s \in \mathcal{S}, n \in \mathcal{N}, n &\notin \mathcal{R}^s \end{aligned} \quad (\text{S2.2})$$

$$\begin{aligned} o_l^s + c_l^s &= a_l^s, \\ \forall s \in \mathcal{S}, l_{a,b} \in \mathcal{L}, l_{a,b} &\in \mathcal{R}^s \end{aligned} \quad (\text{S3.1})$$

$$\begin{aligned} o_n^s + c_n^s &= a_n^s, \\ \forall s \in \mathcal{S}, n \in \mathcal{N}, n &\in \mathcal{R}^s \end{aligned} \quad (\text{S3.2})$$

$$c_l^s = \left\lceil \frac{s.b}{l.s} \right\rceil, \quad (\text{S4.1})$$

$$\forall s \in \mathcal{S}, l_{a,b} \in \mathcal{L}, l_{a,b} \in \mathcal{R}^s$$

$$\begin{aligned} c_n^s &= n.H, \\ \forall s \in \mathcal{S}, n \in \mathcal{N} \cap \mathcal{R}^s, s.secure &= 1 \end{aligned} \quad (\text{S4.2})$$

The cost function we are minimising here ((CS1), (CS2)) is the sum of the end-to-end latencies of all applications, that is, the distance between the start time of the earliest task and the end time of the latest task for each application. The constraint (S1) sets the deadline for the completion of an application to its period. The constraints (S2.1) and (S2.2) set all optimisation variables to zero for every stream, for all nodes and links not part of its route. For all other links and nodes constraints, (S3.1) and (S3.2) set the end-time to be the sum of offset a length. For each link on the route of a stream constraint (S4.1) sets the length to be the byte size of the stream divided by the link speed. In constraint (S4.2) the length of secure streams on end-systems is set to the length of one hash-computation on

that end-system, approximating the duration of MAC generation/verification.

$$\varphi^s > \left\lfloor \frac{a_n^s}{P_{int}} \right\rfloor, \quad (S5)$$

$$\forall s \in S, l_{a,b} \in \mathcal{L} \cap \mathcal{R}^s, b \in \mathcal{E}^s, s.secure == 1$$

$$\begin{aligned} o_n^s &\geq a^{t_{key}} + \varphi^s * P_{int} \\ \forall s \in S, n \in \mathcal{E}^s, s.secure &= 1 \\ \forall t_{key} \in T_{kv}^m \end{aligned} \quad (S6)$$

$$\begin{aligned} a_{l_{a,b}}^s &\leq o_{l_{b,c}}^s \\ \forall s \in S, l_{b,c} &\in \mathcal{L} \cap \mathcal{R}^s \\ a &= x(s, b) \end{aligned} \quad (S7.1)$$

$$\begin{aligned} a_a^s &\leq o_{l_{a,b}}^s \\ \forall s \in S, s.secure &= 1, \\ l_{a,b} &\in \{l_{a,b} | l_{a,b} \in \mathcal{L} \cap \mathcal{R}^s, a = s.t_s.e\} \end{aligned} \quad (S7.2)$$

$$\begin{aligned} a_{l_{a,b}}^s &\leq o_b^s \\ \forall s \in S, s.secure &= 1, \\ l_{a,b} &\in \{l_{a,b} | l_{a,b} \in \mathcal{L} \cap \mathcal{R}^s, b \in \mathcal{E}^s\} \end{aligned} \quad (S7.3)$$

In constraint (S5), the earliest authentication interval for a stream  $\varphi^s$  is bound to be after the latest stream transmission interval. In constraint (S6), the start time of the stream on any receiver end-system is then bound to be greater or equal to the start time of that interval plus the end-time of the necessary preceding key verification task. The constraints (S7.1), (S7.2) and (S7.3) make sure that every stream is scheduled consecutively along its route. Thus, constraint (S7.1) enforces the precedence among two links, (S7.2) among the MAC generation on the sender and the first link and (S7.3) among the last link and the following MAC verification.

$$\begin{aligned} (\alpha \times s_1.T + a_l^{s_1} \leq \beta \times s_2.T + o_l^{s_2}) \quad \vee \\ (\beta \times s_2.T + a_l^{s_2} \leq \alpha \times s_1.T + o_l^{s_1}) \\ \forall s_1, s_2 \in S, s_1 \neq s_2, \forall l \in \mathcal{R}_1^s \cap \mathcal{R}_2^s, \\ \forall \alpha \in \{0, \dots, \text{lcm}(s_1.T, s_2.T)/s_1.T\}, \\ \forall \beta \in \{0, \dots, \text{lcm}(s_1.T, s_2.T)/s_2.T\} \end{aligned} \quad (S8)$$

$$\begin{aligned} (\alpha \times s_2.T + o_{l_{b,c}}^{s_2} \leq \beta \times s_1.T + o_{l_{a_1,b}}^{s_1}) \quad \vee \\ (\beta \times s_1.T + o_{l_{b,c}}^{s_1} \leq \alpha \times s_2.T + o_{l_{a_2,b}}^{s_2}) \\ \forall s_1, s_2 \in S, s_1 \neq s_2, \forall l \in \mathcal{R}_1^s \cap \mathcal{R}_2^s, \\ a_1 = x(s_1, b), a_2 = x(s_2, b), \\ \forall \alpha \in \{0, \dots, \text{lcm}(s_1.T, s_2.T)/s_1.T\}, \\ \forall \beta \in \{0, \dots, \text{lcm}(s_1.T, s_2.T)/s_2.T\} \end{aligned} \quad (S9)$$

The constraint (S8) prevents any streams from overlapping on any nodes or links. Furthermore, constraint (S9)

guarantees that for each link connected to an output port of a switch, the frames arriving on all input ports of that switch that want to use this output port cannot overlap in the time domain. This is the frame isolation necessary for determinism in our TSN configuration, which is further explained in Ref. [5].

$$o^t + t.w = a^t, \forall t \in \mathcal{T} \quad (T1)$$

$$\begin{aligned} a^t &\leq o_{t,e}^s \\ \forall t \in \mathcal{T}, s \in S, s.t_s = t, s.secure &= 1 \end{aligned} \quad (T2.1)$$

$$\begin{aligned} a^t &\leq o_{l_{a,b}}^s \\ \forall t \in \mathcal{T}, s \in S, s.t_s = t, s.secure &= 0 \\ \forall l_{a,b} \in \mathcal{L} \cap \mathcal{R}^s, a &= t.e \end{aligned} \quad (T2.2)$$

$$\begin{aligned} a_{t,e}^s &\leq o^t \\ \forall t \in \mathcal{T}, s \in S, t \in s.T_d, s.secure &= 1 \end{aligned} \quad (T3.1)$$

$$\begin{aligned} a_{l_{a,b}}^s &\leq o^t \\ \forall t \in \mathcal{T}, s \in S, t \in s.T_s, s.secure &= 0 \\ \forall l_{a,b} \in \mathcal{L} \cap \mathcal{R}^s, b \in \mathcal{E}^s \end{aligned} \quad (T3.2)$$

$$\begin{aligned} (\alpha \times t_1.T + a^{t_1} \leq \beta \times t_2.T + o^{t_2}) \quad \vee \\ (\beta \times t_2.T + a^{t_2} \leq \alpha \times t_1.T + o^{t_1}) \\ \forall t_1, t_2 \in \mathcal{T}, t_1 \neq t_2, \\ \forall \alpha \in \{0, \dots, \text{lcm}(t_1.T, t_2.T)/t_1.T\}, \\ \forall \beta \in \{0, \dots, \text{lcm}(t_1.T, t_2.T)/t_2.T\} \end{aligned} \quad (T4)$$

$$\begin{aligned} (\alpha \times t.T + a^t \leq \beta \times s.T + o_{t,e}^s) \quad \vee \\ (\beta \times s.T + a_{t,e}^s \leq \alpha \times t.T + o^t) \\ \forall t \in \mathcal{T}, s \in S, s.secure = 1, t.e \in \mathcal{R}^s \\ \forall \alpha \in \{0, \dots, \text{lcm}(t.T, s.T)/t.T\}, \\ \forall \beta \in \{0, \dots, \text{lcm}(t.T, s.T)/s.T\} \end{aligned} \quad (T5)$$

The constraint (T1) sets the end-time of a task to be the sum of offset and length. The constraints (T2.1) and (T2.2) model the dependency between a task and all its outgoing streams: such streams may only start after the task has finished. Similarly, constraints (T3.1) and (T3.2) model the dependency between a task and its incoming streams: such a task may only start after all incoming streams have arrived. Finally, constraint (T4) prevents any two tasks from overlapping, while constraint (T5) prevents a task from overlapping with a MAC generation/verification operation.

## 7 | METAHEURISTIC FORMULATION

As mentioned in Section 6, the scheduling problem addressed in this paper is NP-hard. As a consequence, a pure CP formulation solved using a CP solver is not tractable for large problem sizes. Hence, in this section, we propose a metaheuristic-based strategy, which aims to find good

solutions (without the guarantee of optimality) in a reasonable time, even for large test cases.

An overview of our strategy is presented in Algorithm 1. We use a Simulated Annealing (SA) metaheuristic [45] to find solutions  $\Phi = (\mathcal{R}, \Sigma)$ , consisting of a set of routes  $\mathcal{R}$  and a schedule  $\Sigma$ . As an input, we provide our architecture model  $(\mathcal{N}, \mathcal{L})$  and the application model  $\Lambda$ . SA randomly explores the solution space in each iteration by generating “neighbours” of the current solution using design transformations (or ‘moves’). We consider both routing and scheduling-related moves, and the choice is controlled by a  $p_{rmv}$  parameter that gives the probability of a routing move. To measure the quality of a solution, we use a cost function with two parameters,  $a$  and  $b$ , which are factors for punishing overlap of redundant streams and missed deadlines for applications, respectively. While we always accept better solutions, the central idea of Simulated Annealing is to also accept worse solutions with a certain probability in order not to get stuck in local optima [46].

Algorithm 1 shows the main loop of the heuristic. We start out with an initial solution, a cost value, and a positive temperature (line 2–4). Then, we repeat the steps described below until a stopping criterion such as a time- or iteration-limit is met. We create a slight permutation of the current solution  $\Phi$  by using the *RandomNeighbour* function (line 6). We calculate the cost of the new solution (line 7) and a delta of the new and old cost (line 8). Now, if the delta is smaller than 0, that is, if  $\Phi_{new}$  is a better solution than  $\Phi$ , we choose  $\Phi_{new}$  as the current solution (line 10–12). Alternatively, the new solution is also accepted if a randomly chosen value between 0 and 1 is smaller than the value of the acceptance probability function  $e^{-\frac{\delta}{t}}$ . This acceptance probability will decrease with the temperature over time and is also influenced by  $\delta$ , which gives a measure of how much worse the new solution is. Finally, since we will occasionally accept worse solutions, we keep track of the best cost achieved overall and adjust it if necessary (line 12–14).

### Algorithm 1 Simulated Annealing Metaheuristic

```

1 Function heuristic( $\mathcal{N}, \mathcal{L}, \Lambda, T_{start}, \alpha, k, p_{rmv}, a, b, w$ )
2    $\Phi_{best} = \Phi = \text{InitialSolution}(\mathcal{N}, \mathcal{L}, \Lambda, k)$ ;
3    $c_{best} = c = \text{Cost}(\Phi, a, b)$ ;
4    $t = T_{start}$ ;
5   while stopping-criterion not True do
6      $\Phi_{new} = \text{RandomNeighbour}(\Phi, p_{rmv})$ ;
7      $c_{new} = \text{Cost}(\Phi_{new}, a, b)$ ;
8      $\delta = c_{new} - c$ ;
9     if  $\delta < 0$  or random[0,1)  $< e^{-\frac{\delta}{t}}$  then
10       $\Phi = \Phi_{new}$ ;
11       $c = c_{new}$ ;
12      if  $c_{new} < c_{best}$  then
13         $\Phi_{best} = \Phi_{new}$ ;
14         $c_{best} = c_{new}$ ;
15       $t = t * \alpha$ ;
16   end
17   return  $\Phi_{best}$ ;

```

## 7.1 | Precedence graph

We introduce a helper data structure in the form of a precedence graph. A precedence graph is a collection of special DAGs, one for each application. These DAGs are expanded versions of the DAGs from the application model. Here, streams are modelled as nodes instead of edges, and each redundant copy of a stream has its own node. See Figure 7 for an example. This data structure helps to model all the dependencies between tasks and streams in the scheduling algorithm. Additionally, we will use the set of all topological orders of this graph as our solution space for the scheduling step. An order can be seen as a scheduling priority assignment that respects all precedence constraints.

## 7.2 | Initial solution

### Algorithm 2 Initial Solution

```

1 Function InitialSolution( $\mathcal{N}, \mathcal{L}, \Lambda, k, w$ )
2   // routing
3   foreach  $s \in \mathcal{S}$  do
4     foreach  $e_r \in \{t_r.e | t_r \in s.T_d\}$  do
5       if IsFirstCopyOfStream( $s$ ) then
6          $K_s^{e_r} = \text{ShortestPaths}(s.t_s.e, e_r, k, \mathcal{N}, \mathcal{L})$ ;
7       else
8          $K_s^{e_r} =$ 
9            $\text{ShortestPathsWeighted}(s.t_s.e, e_r, k, \mathcal{N}, \mathcal{L}, w)$ ;
10       $\Phi.R^s = \text{ShortestPath}(K_s^{e_r})$ ;
11   end
12   // schedule
13    $P = \text{CreatePrecedenceGraph}(\Lambda)$ ;
14   foreach  $\lambda_s \in \Lambda^{sec}$  do
15      $O = O \cup \text{TopologicalOrder}(\lambda_s, P)$ ;
16   end
17   foreach  $\lambda_n \in \Lambda \setminus \Lambda^{sec}$  do
18      $O = O \cup \text{TopologicalOrder}(\lambda_n, P)$ ;
19   end
20    $\Phi.K = K$ ;  $\Phi.P = P$ ;  $\Phi.O = O$ ;
21    $\Phi.\Sigma = \text{Schedule}(O, \Phi.R)$ ;
22   return  $\Phi$ ;

```

In the beginning, we create an initial solution  $\Phi$  from the given architecture and application model. A solution is a tuple  $(\mathcal{R}, \Sigma)$  consisting of a set of routes  $\mathcal{R}$  and a schedule  $\Sigma$ . Algorithm 2 details the function to find the initial solution.

To find an initial set of routes, we iterate through all streams and all pairs of sender and receiver ES (lines 2–3). For each such pair, we calculate and store  $k$  shortest paths for the given topology (line 5). For each redundant copy of a stream beyond the first, we calculate the shortest path in a weighted graph, where we weight all links used by previous copies with  $w$  instead of 1 (line 7). For the initial solution, we choose the shortest path for each pair (line 8).

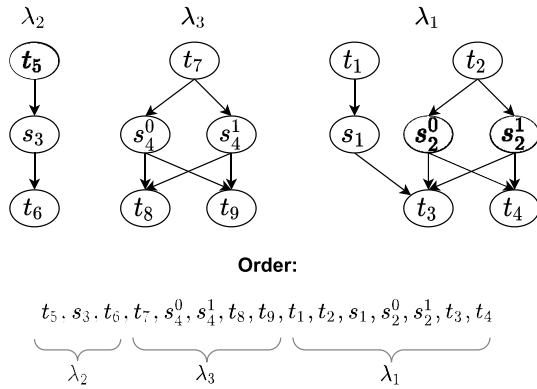


FIGURE 7 Example precedence graph with the associated order

Note that our k-shortest-path algorithm only generates paths without repeated nodes that do not traverse any end-system.

To find an initial schedule, we have to create the precedence graph  $P$  (line 11) and decide an order  $O$  of this graph.

For the initial solution, we construct an order on the level of applications, that is, we avoid interleaving nodes of different applications. We prioritise key applications (lines 12–14) before other (normal) applications (lines 15–17). This order is consequently used to create a schedule (line 19). See Figure 7 for an example order.

### 7.3 | Neighbourhood function

#### Algorithm 3 RandomNeighbour

```

1 Function RandomNeighbour( $\Phi, p_{rmv}$ )
2    $p = \text{random}[0, 1]$ ;
3   if  $p < p_{rmv}$  then
4      $s = \text{RandomStream}(\Phi)$ ;
5      $e_r = \text{RandomReceiver}(s)$ ;
6      $\Phi.\mathcal{R}^s = \text{RandomPath}(\Phi, K_s^{e_r})$ ;
7   else
8      $d_1 = \text{RandomNormalApplication}(\Phi)$ ;
9      $d_2 = \text{RandomNormalApplication}(\Phi)$ ;
10     $\Phi.O = \text{SwitchSchedulingOrder}(d_1, d_2, \Phi.O)$ ;
11     $\Phi.\Sigma = \text{Schedule}(\Phi.O, \Phi.\mathcal{R})$ ;
12     $\Phi.\Sigma = \text{OptimizeLatency}(\Phi.\Sigma, \Phi.P)$ ;
13  end
14  return  $\Phi$ ;

```

The neighbourhood function  $\text{RandomNeighbour}(\Lambda, p_{rmv})$  is detailed in Algorithm 3. It is used during Simulated Annealing to create a slight permutation of a given solution/candidate  $\Phi$ . It contains two fundamental moves: Changing the routing  $\Lambda.\mathcal{R}$  or changing the schedule  $\Lambda.\Sigma$ . Which move is taken is decided randomly (line 3). The parameter  $p_{rmv}$  influences how likely it is that the routing move is taken, for example,  $p_{rmv} = 0.5$  would result in a probability of 50%.

A routing move consists of choosing a random stream  $s$  out of the set of all streams (line 4), choosing a random receiver  $e_r$  out of all receivers of that stream (line 5) and then assigning a random path out of the set of k-shortest-paths calculated during the creation of the initial solution (line 6).

A scheduling move consists of choosing two random normal (non-key) applications  $d_1$  and  $d_2$  (lines 8 and 9), switching their order  $O$  in the precedence graph  $P$  (line 10) and recalculating the schedule (line 11). Whenever a new schedule is calculated, we also optimise its latency (line 12). This is further explained in Section 7.7.

### 7.4 | Cost function

The cost function is used in the simulated annealing meta-heuristic to evaluate the quality of a solution. A lower cost means a better solution. Algorithm 4 shows how our cost function is calculated. It consists of two components: a routing cost  $c_{\text{route}}$  and a schedule cost  $c_{\text{sched}}$ . The routing cost is the sum of the number of overlaps of the redundant stream (one for each stream for each link), which is punished with a factor  $a$  and the total accrued length of all routes. The schedule cost is the sum of the number of infeasible applications, which is punished with a factor  $b$ , and the total sum of all application latencies (distance between start-time of first task and end-time of the last task). The factors  $a$  and  $b$  should be sufficiently high such that solutions with less overlap and infeasible applications are preferred.

#### Algorithm 4 Cost

```

1 Function Cost( $\Phi, a, b$ )
2    $c_{\text{route}} = a * \text{Overlaps}(\Phi.\mathcal{R}) + \text{Length}(\Phi.\mathcal{R})$ ;
3    $c_{\text{sched}} = b * \text{Infeasible}(\Phi.\Sigma) + \text{Latency}(\Phi.\Sigma)$ ;
4   return  $c_{\text{route}} + c_{\text{sched}}$ ;

```

### 7.5 | ASAP list scheduling

To calculate a schedule for a given precedence graph with associated order and routing, we use an ASAP list-scheduling heuristic [47], which schedules each node of the precedence graph in the given order.

The algorithm, presented in Algorithm 5, starts by iterating through each entry  $n$  of the given order  $O$  (line 2). An entry may either be a task or a stream. For each entry, we determine where it will be scheduled and create an indexable list  $L$  with all these locations (line 3). For a task, that set would contain just one end-system, while for a stream, it may contain many links (which are synonymous to an output port of a switch/ES) and also multiple end-systems, if the stream is secure, thus requiring MAC generation/verification.

Using these locations we also create a set of blocks (line 4). A block  $b$  is a tuple  $(e, l, o, \bar{o}, prev, next)$  that is associated to an entry  $e$  (task/stream) and a location  $l$  (node/link).  $o$  represents the block offset.  $\underline{o}$  and  $\bar{o}$  are parameters representing

a lower and upper bound on the offset, which are used during the algorithm. The set  $B$  is implemented as a linked list, where  $prev$  and  $next$  are references to neighbouring blocks on the route  $L$ . Note that in the case of multicast streams  $next$  could contain references to multiple blocks.

### Algorithm 5 Scheduling—ASAP Heuristic

```

1 Function  $Schedule(P, \mathcal{R})$ 
2   foreach  $n \in \mathcal{O}$  do
3      $L = \text{GetRoute}(n, \mathcal{R});$ 
4      $B = \text{CreateBlocks}(n, L);$ 
5      $l = L[0];$ 
6      $i = 0;$ 
7     while true do
8        $b = B[l];$ 
9        $b.o = \text{CalculateLowerBound}(n, b, P, \mathcal{R});$ 
10       $o = \text{EarliestOffset}(b, l);$ 
11      if  $o == \infty$  then
12        return false;
13      else if  $o \leq b.o$  then
14         $b.o = o;$ 
15        foreach  $g \in b.next$  do
16          if  $\text{IsBlockOnLink}(g)$  then
17             $g.o =$ 
18               $\text{LatestQueueAvailableTime}(g, o);$ 
19          end
20           $i = i + 1;$ 
21          if  $i < \text{len}(L)$  then
22             $l = L[i];$ 
23          else
24            break;
25          end
26        else
27           $g = b.prev;$ 
28           $g.o = \text{EarliestQueueAvailableTime}(b, o);$ 
29           $l = b.prev.l;$ 
30           $i = L.\text{indexOf}(l);$ 
31        end
32      end
33       $\Sigma = \text{UpdateSchedule}(n);$ 
34    end
return  $\Sigma;$ 

```

We now iterate over all these blocks (lines 7–8). For each block we begin by calculating the lower bound on the offset (line 9).<sup>2</sup> Usually, this lower bound is going to be the end-time (offset + length) of the block on the previous link, making sure that a stream is scheduled consecutively along its route. The first block is the maximum of all end-times of the last blocks of the predecessors of the current entry  $n$  in the precedence graph. For example, for application  $\lambda_1$  in Figure 7, the lower bound of the offset of the block of  $t_3$  would be set to the maximum of the end-times of the last blocks of  $s_1$ ,  $s_2^0$  and  $s_2^1$ .

Also, for a secure stream, for all blocks on receiver ESs (i.e., MAC validation tasks), the lower bound is set to the end-time of the corresponding key verification task in the TESLA interval after the stream was received on the ES, since, according to the TESLA security condition, the stream can only be authenticated from that point on.

In the next step, the earliest possible offset for the current block is calculated (line 10). This function returns the earliest offset greater or equal to the lower bound within the feasible region. For more detail see Section 7.6.

If such an offset is found and it is smaller than or equal to the upper bound, we can assign it to the block (line 14). We then iterate through each of the following blocks and set their upper bound to the latest point in time when their node is available and has been since the offset (line 15–18). This is carried to fulfil the TSN constraint, which forbids different streams to interleave within a queue (c.f. [5, 48] for a more detailed explanation).

If such an offset is found but it is larger than the upper bound, it is impossible to schedule the block while the port is still available, that is, without it interleaving with other streams (line 25). Consequently, we have to backtrack and schedule the previous block at a later time. Therefore we set the lower bound of the previous block to the earliest time when the current port is available and remains so until the offset (line 26–27).

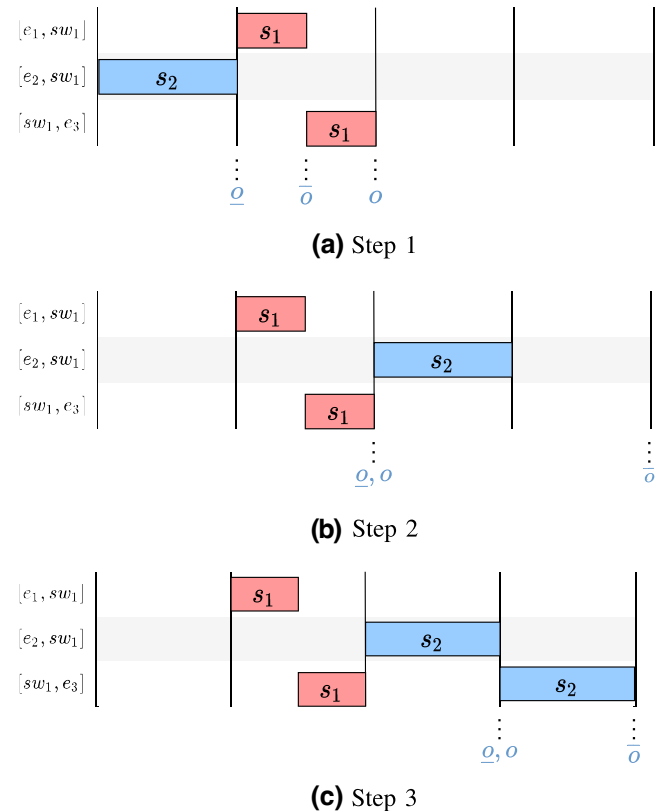


FIGURE 8 Backtrack example: Scheduling  $s_2$

<sup>2</sup>The algorithm can be found in Appendix B

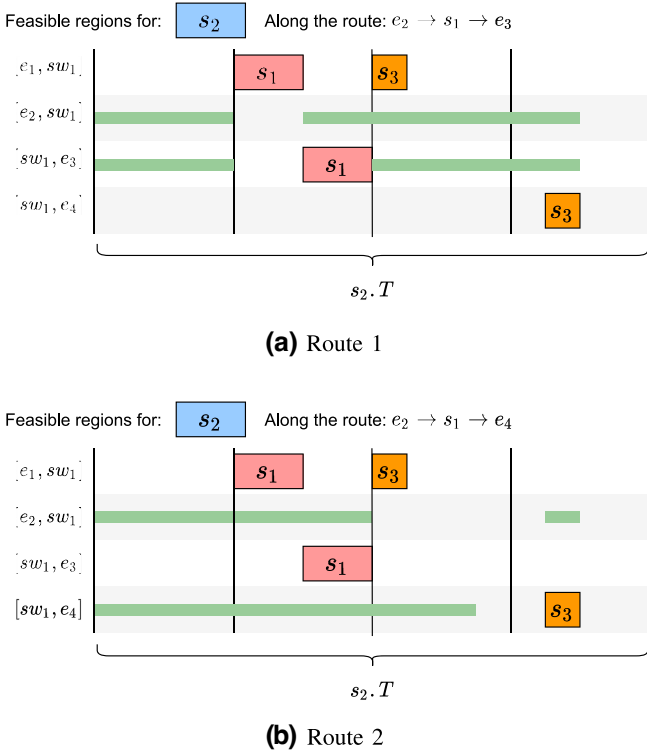


FIGURE 9 Feasible region example

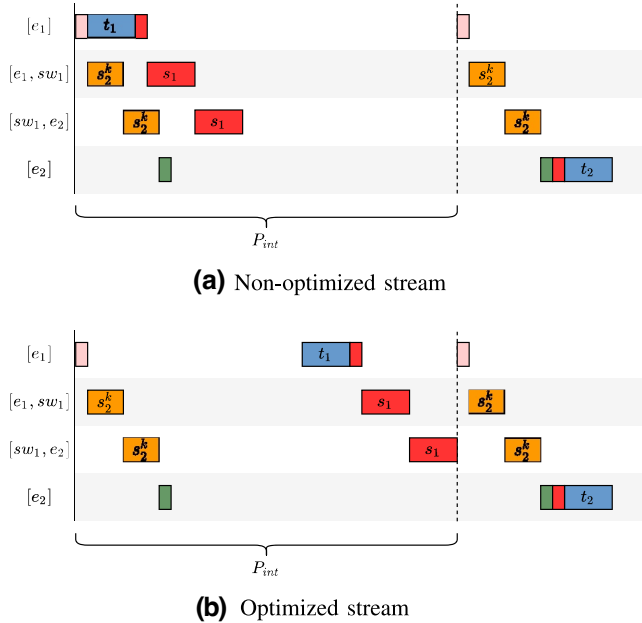


FIGURE 10 Latency optimisation for secure streams

Figure 8 gives an example of this process. In step 1,  $s_1$  has already been scheduled, and we are in the process of scheduling  $s_2$ . We have scheduled the first block on  $l_{e_2, sw_1}$  and are now trying to schedule the second one on  $l_{sw_1, e_3}$ . The lower bound of our offset  $o$  is set to the end-time of the first block. The upper bound  $\bar{o}$  is set to the latest time after which  $l_{sw_1, e_3}$  is still available after the offset of the first block, that is,

the start time of  $s_1$  on that link. Finally, we find the earliest offset  $o$  to be only after the end time of  $s_1$ . It cannot be earlier since then the blocks of  $s_2$  and  $s_1$  would overlap. However, scheduling  $s_2$  at that time is not possible since it would mean that the two streams interleave at the same port. Consequently, in step 2, we backtrack and reschedule the first block of  $s_2$  by setting the lower bound on its offset to the earliest time when its port is available and remains so until  $o$ . In step 3, we are able to schedule the second block of  $s_2$  without problems.

Once we have successfully found an offset for each block, we can update the schedule (line 32). This will remove the found blocks  $B$  from the feasible region.

## 7.6 | Calculating the earliest offset

Calculating the earliest offset for a given block is an important part of the heuristic. Algorithm 6 shows the function. It takes a block  $b$  as an input and calculates the feasible region for that block (line 2). It then returns the lowest possible time that is within the feasible region and greater or equal than the lower bound (lines 3–6).

### Algorithm 6 ASAP Heuristic—EarliestOffset

```

1 Function EarliestOffset( $b$ )
   /* ordered set of intervals */
2    $I = \text{GetFeasibleRegion}(b)$ ;
3   foreach  $i \in I$  do
4      $o = \max(b.o, i.\text{begin})$ ;
5     if  $i.\text{contains}(o)$  then
6       return  $o$ ;
7   end

```

The function to calculate the feasible regions for a given block  $b$  is detailed in Algorithm 7. We start by getting all free intervals on the node/link  $b.l$  for the period  $b.e.T$  of the block (line 3). This ensures that the feasible region does not include any previously scheduled blocks on that node/link. The function then proceeds to fill the data structure  $R_{\text{feas}}$  with the free intervals while cutting off a piece with the length of the block  $b$  from the end of each such interval (lines 4–7). This makes the feasible region represent all feasible values for the offset of the block.

If the block is assigned to a link, we have to cut down the feasible region further. Due to the TSN isolation constraint, it is not allowed to transmit two different streams on the same port at the same time. Thus, we iterate here over all the subsequent blocks  $b_{\text{next}}$  of the current block  $b$ , that is, the blocks on the next links/ES on the route of the stream associated with the block (line 9). If the next block is also assigned to a link (not to an ES), we iterate through all already scheduled blocks  $b_{\text{other}}$  on that link  $b_{\text{next}.l}$ . These are blocks from other streams with whose predecessors, wherever

TABLE 3 Scalability tests

Test case	Method	# ES	# SW	# Streams	# Recv. Tasks	# Tasks	Cost	T
Example	CP	4	2	6	10	9	467	1 s
Example	SA	4	2	6	10	9	477	10 m
Auto	CP	20	32	84	102	74	/	/
Auto	SA	20	32	84	102	74	38,031	10 m
Case_study	CP	6	2	29	31	28	3771	130 s
Case_study	SA	6	2	29	31	28	6114	10 m
Tiny1	CP	4	2	2	2	6	1708	0.2 s
Tiny1	SA	4	2	2	2	6	1708	10 m
Tiny2	CP	4	2	3	4	6	1732	0.2 s
Tiny2	SA	4	2	3	4	6	1732	10 m
Tiny3	CP	4	2	11	13	15	7450	14 m
Tiny3	SA	4	2	11	13	15	18,088	10 m
Small1	CP	8	4	10	16	20	5421	2 s
Small1	SA	8	4	10	16	20	13,303	10 m
Small2	CP	8	4	14	20	23	9110	60 m
Small2	SA	8	4	14	20	23	13,794	10 m
Small3	CP	8	4	29	48	35	7705	17.5 m
Small3	SA	8	4	29	48	35	13,781	10 m
Medium1	CP	16	8	23	34	37	12,991	4.5 m
Medium1	SA	16	8	23	34	37	22,883	10 m
Medium2	CP	16	8	30	47	43	6552	5.2 m
Medium2	SA	16	8	30	47	43	19,455	10 m
Medium3	CP	16	8	36	53	47	15,515	60 m
Medium3	SA	16	8	36	53	47	26,486	10 m
Large1	CP	32	16	47	86	73	/	/
Large1	SA	32	16	47	86	73	43,872	10 m
Large2	CP	32	16	33	65	72	24,953	25 m
Large2	SA	32	16	33	65	72	41,026	10 m
Large3	CP	32	16	69	170	104	/	/
Large3	SA	32	16	69	170	104	34,860	10 m
Huge1	CP	64	32	84	183	133	/	/
Huge1	SA	64	32	84	183	133	73,070	10 m
Huge2	CP	64	32	99	213	161	/	/
Huge2	SA	64	32	99	213	161	57,246	10 m
Huge3	CP	64	32	99	197	169	/	/
Huge3	SA	64	32	99	197	169	93,357	10 m
Giant1	CP	128	64	144	347	261	/	/
Giant1	SA	128	64	144	347	261	101,799	20 m



they are scheduled, we are not allowed to overlap. Thus, we cut the interval  $(b_{other\text{-}prev.o}, b_{other.o})$  from the feasible region (line 13).

### Algorithm 7 ASAP Heuristic—GetFeasibleRegion

```

1 Function GetFeasibleRegion(b)
2    $R_{feas} = \emptyset$ ;
3    $B_{free} = \text{GetFreeIntervals}(b.l, b.e.T)$ ;
4   /* (i) Add all free intervals that could
   contain block b */
5   foreach  $iv \in B_{free}$  do
6     if  $iv.end - \text{Length}(b) \geq iv.begin$  then
7        $R_{feas} = \text{AddToFeasibleRegion}(R_{feas},$ 
8          $(iv.begin, iv.end - \text{Length}(b)))$ ;
9     end
10  if  $\text{IsLink}(b.l)$  then
11    /* (ii) Cut out the interval blocked by
12    other streams on the next port (TSN
13    Stream Isolation) */
14    foreach  $b_{next} \in b.next$  do
15      if  $\text{IsLink}(b_{next}.l)$  then
16        foreach
17           $b_{other} \in \text{GetAllBlocksForLink}(b_{next}.l)$  do
18          if  $b_{other} \neq b_{next}$  then
19             $R_{feas} =$ 
20               $\text{CutFromFeasibleRegion}(R_{feas},$ 
21                 $(b_{other}.prev.o, b_{other}.o))$ ;
22          end
23        end
24    end
25  return  $R_{feas}$ ;

```

Figure 9 provides two examples of feasible regions, shown in green, for a stream  $s_2$  on two different routes. Looking at Figure 9a, note the free space at the end of the period and before  $s_1$  on  $l_{sw_1, e_3}$ . Choosing an offset anywhere in this space would result in  $s_2$  being scheduled outside its period or overlapping with  $s_1$ . Choosing an offset in the first free space on  $l_{e_2, sw_1}$  would result in  $s_1$  and  $s_2$  being transmitted to the same port at the same time, breaking the TSN isolation constraint. Note how in Figure 9b this is not the case, since  $s_2$  is transmitted to a different port ( $l_{sw_1, e_4}$ ) than  $s_1$ .

## 7.7 | Optimising the latency for secure streams

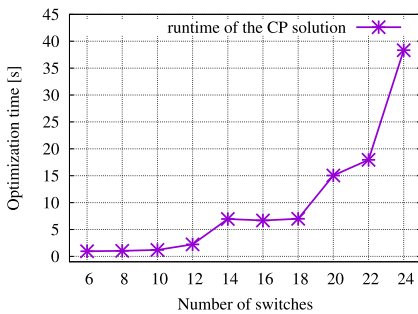
After we have created a new schedule, we can apply some post-processing to minimise its latency. Since TESLA requires a separation of sending and receiving tasks into separate intervals and since we are using an ASAP heuristic, there can be a significant gap between those tasks, as can be seen in Figure 10a, resulting in an increased latency. To minimise the latency, the algorithm in Algorithm 8 will go through each secure stream of each application (line 4). It will use the *OptimizeLatencyForSecureStream* function in Algorithm 9 to optimise each stream individually. This function shifts all instances of the given stream as close to the instances on the receiver end-system as possible without breaking the TESLA constraint. It also has an optional Boolean parameter. If that is set, it also shifts the sending task of the given stream (otherwise, there would be no latency gain). However, when we are optimising a redundant stream, that is, a stream where multiple copies originate at the same task, the said task should only be moved when the last copy is optimised (lines 6–11). Otherwise, we can shift it immediately (line 13).

### Algorithm 8 ASAP Heuristic—OptimizeLatency

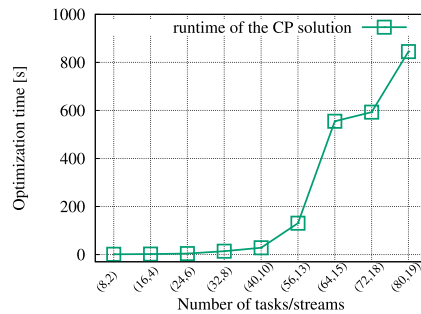
```

1 Function OptimizeLatency( $\Sigma, P$ )
2   foreach  $\lambda \in \Lambda$  do
3     foreach  $n \in \text{TopologicalOrder}(\lambda, P)$  do
4       if  $\text{IsStream}(n.e)$  and  $n.e.secure$  and  $n.e \in S^d$ 
5         then
6           if  $n.e.rl > 1$  then
7             foreach  $s_r \in S_{n.e}$  do
8               if  $s_r \neq n.e$  then
9                  $n_r = \text{GetNode}(s_r, P)$ ;
10                 $\text{OptimizeLatencyForStream}(n_r,$ 
11                   $\text{False})$ ;
12              end
13             $\text{OptimizeLatencyForStream}(n.e, \text{True})$ ;
14          else
15             $\text{OptimizeLatencyForStream}(n, \text{True})$ ;
16        end
17      end
18    end

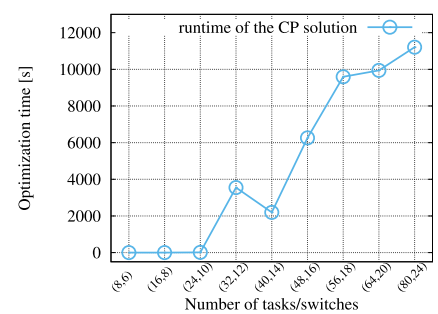
```



(a) Impact of topology size (Set A)



(b) Impact of task/stream amount (Set B)



(c) Impact of both combined (Set C)

FIGURE 11 Scalability of CP solution

The *OptimizeLatencyForSecureStream* function in Algorithm 9 works internally by looping through the list of receivers of the given stream (line 2, multiple in case of a multicast stream). It goes backwards through the linked list of blocks for the stream, starting with the block on the last link before the current receiver (line 4). For each block, it will increase the offset as much as possible (move them as far as possible to the right; line 10). After changing the offset we update the schedule (line 11). Then we continue iterating through the linked list (lines 17–19). If we arrive at the last block and the *move\_task* Boolean is set, we finish by the offset of the sender task (lines 12–16).

### Algorithm 9 ASAP Heuristic—OptimizeLatency-ForStream

```

1 Function OptimizeLatencyForStream(n, move_task)
2   foreach  $es_{recv} \in receivers(n)$  do
3      $b = \text{BlockOnLink}(es_{recv}, n);$ 
4      $b_{prev} = b.prev;$ 
5      $t_{kv} = \text{GetKeyVerificationTask}(n.src, e);$ 
6      $b_{kv} = \text{GetBlock}(t_{kv});$ 
7      $i = \text{GetTESLAIntervalForBlock}(b_{kv});$ 
8      $ub = i * t_{kv}.T - b_{prev}.L;$ 
9     while  $b_{prev} \neq \emptyset$  do
10       $b_{prev}.o = \min(ub, b_{prev}.o);$ 
11       $\text{UpdateSchedule}(n);$ 
12      if  $b_{prev}.prev == \emptyset$  and move_task and
13         $\text{IsLastReceiver}(es_{recv})$  then
14        /* Also move the sender task closer
15         to the first block of the stream
16         */
17         $t_{sender} = \text{GetSenderTask}(n);$ 
18         $b_{sender} = \text{GetBlock}(t_{sender});$ 
19         $ub = b_{prev}.o - b_{sender}.L;$ 
20         $b_{prev} = t_{sender};$ 
21      else if  $b_{prev}.prev \neq \emptyset$  then
22         $ub = b_{prev}.o - b_{prev}.prev.L;$ 
23         $b_{prev} = b_{prev}.prev;$ 
24      end
25    end

```

## 8 | EXPERIMENTAL RESULTS

In this section, we evaluate our two solutions to the formulated problem: The Constraint Programming formulation (referred to as *CP*, described in Section 6) and the Simulated Annealing metaheuristic (referred to as *SA*, described in Section 7). We analyse their scalability, runtime and solution quality and evaluate the impact of added redundancy and security.

Both solutions were implemented in Python 3.9. We developed a software tool with a web-based interactive user interface to display the models and solutions, including a routing graph and the schedule.<sup>3</sup> For solving the CP

formulation, we use the CP-SAT solver from Google OR-Tools [49]. For calculating k-shortest-paths in the metaheuristic we use the *shortest\_simple\_paths* function from the NetworkX [50] library. All evaluations were run on a High-Performance Computing (HPC) cluster, where each node is comprised of two Intel Xeon 2660v3 Processors with 10 cores running at 2.60 GHz and 16 GB memory. Both CP and SA run on one node at a time.

### 8.1 | Test cases used for the evaluation

For the scalability evaluation we used the following test cases, see Table 3, the example presented in Section 5 (*example*), a realistic automotive test case from a large automotive manufacturer (*auto*) [6], a medium-sized automotive case study from Ref. [51] (*case\_study*) and 16 synthetic test cases of increasing size and complexity. The topology of the auto test case was adjusted to allow disjunct redundant routes.

For the redundancy/security impact evaluation, we used an additional set of 100 synthetic test cases grouped into four batches.

We created the synthetic test cases to be as realistic as possible: They all feature secure streams, redundancy levels between 1 and 3, applications with complex dependencies and a realistic network topology that allows disjunct redundant paths.

To create realistic topologies, we developed a custom algorithm as follows. For a given number of switches and end-systems, we create that many random points in 2-D space. Then we connect each switch to its closest neighbour until every switch is connected to four other switches. Afterwards, we connect each end-system to the closest three switches.

To create realistic application DAGs, we used the GGen tool presented in Ref. [52] and the layer-by-layer method with a depth of 3 and a connection probability of 50%. If a DAG contains separate subgraphs, these are split into separate applications. The application period is chosen randomly among the set {10, 15, 20, 50 ms}. Nodes of the generated DAG are interpreted as tasks with a random WCET, upper bound at 6% of the period. Tasks are divided randomly between ES. All outgoing edges of a node in the DAG combined are interpreted as a stream, with the source node as the sender task and the destination nodes as receiver tasks. The stream has a random size below or equal to 1.500 Bytes, with a random RL between 1 and 3 and a 30% probability to be considered security-critical.

We used a link speed of 1000 Mbit/s for all links in the network. TESLA uses 16 B keys and MACs, and a hash computation takes 10  $\mu$ s on every ES.

### 8.2 | Scalability evaluation

To evaluate the scalability, we ran both the CP and the SA solutions on the same test cases with the same computing resources. Table 3 shows the results for each test case for both

<sup>3</sup>The tool including the obtained results is available on GitHub: <https://github.com/nreusch/TSNConf>.

solutions. The columns **# ES**, **# SW**, **# Streams**, and **# Tasks** give the total number of ES, SW, streams, and tasks, respectively. **# Receiver Tasks** gives the total sum of stream receiver tasks (since we consider multicast streams, one stream can have multiple). The **Cost** column gives the total cost of the found solution following the cost function in Algorithm 4. The **T** column shows the total runtime of the solver.

The CP solution was given a timeout of 60 min. If CP failed to find an optimal solution in time, or ran out of memory, we reported Cost and T as empty '/'. The SA solution was given a timeout of 10 min (20 min for the largest test case, giant1). We used ParamILS [53] to optimise the following parameters for the SA heuristic:  $T_{\text{start}}$ ,  $\alpha$ ,  $k$ ,  $p_{mv}$  and  $w$ .  $a$  was set to 50,000 and  $b$  to 10,000.

Note that the CP solver will return once the optimal solution is found, while the SA solver will always run until the timeout and return the best feasible (i.e., no missed deadlines or overlap) solution found up to that point. However, SA is able to find a first feasible solution very quickly. For all test cases in Table 3 it could find one in less than 10 s.

The table shows that CP is able to find solutions up to medium-sized test cases within the given timeout, but it does not scale to the larger test cases. SA is scalable; it is able to find solutions even for the largest test cases. This scalability comes at an increase in cost by 67% on average, which can be reduced by giving a longer timeout. This increase is mostly caused by increased application latencies (scheduling cost), which are still within the deadlines, while the routing cost is usually close to or equal to the optimal routing cost from the CP solution. The

conclusion is that SA can be successfully used to route and schedule large realistic test cases, and its quality is comparable to the optimal solutions obtained by CP.

Furthermore, we have investigated the impact of scaling different parameters on the runtime of the CP solution. We created three sets of test cases: The set **A**, used in Figure 11a, in which we keep a fixed set of applications but scale the size of the network topology, the set **B**, used in Figure 11b, in which we keep a fixed network topology and scale the number of tasks, and streams and the set **C**, used in Figure 11c in which we scale both at the same time. We ran the tests on the same computing resources and took the average runtime of multiple runs to reduce the impact of external factors (disk access, caching etc.). While, as expected, all the parameters have a measurable impact on runtime, we noticed that the number of streams and the complexities of their routes have a significant impact as can also be seen in Figure 11b.

### 8.3 | Impact of adding redundancy and security to a test case

Fulfilling the security and redundancy requirements of applications introduces extra tasks and streams that need to be routed and scheduled, leading to an overhead compared to ignoring those security and redundancy requirements. In this set of experiments, we were interested in evaluating the overhead of fulfilling the redundancy and security requirements compared to the case these are ignored. These overheads were measured on solution cost, available bandwidth, and CPU

Batch name	Security	Redundancy	Cost	Bandwidth	CPU
0 Batch0 – large streams, small tasks	No	No	3822.08	0.09	1.44
1	No	Yes	+1.34%	+25.45%	+0.00%
2	Yes	No	+256.25%	+5.49%	+12.99%
3	Yes	Yes	+258.10%	+36.64%	+15.93%
4 Batch1 – large streams, large tasks	No	No	17 721.32	0.08	7.06
5	No	Yes	$\pm 0.00\%$	+15.91%	+0.00%
6	Yes	No	+64.31%	+3.18%	+1.39%
7	Yes	Yes	+64.98%	+22.16%	+1.75%
8 Batch2 – small streams, large tasks	No	No	18 547.6	0.01	7.51
9	No	Yes	+0.06%	+31.29%	+0.00%
10	Yes	No	+52.86%	+33.92%	+0.21%
11	Yes	Yes	+53.12%	+97.96%	+0.70%
12 Batch3 – small streams, small tasks	No	No	3713.32	0.01	1.55
13	No	Yes	+0.37%	+26.62%	+0.00%
14	Yes	No	+238.77%	+27.73%	+8.54%
15	Yes	Yes	+245.32%	+85.57%	+10.57%

TABLE 4 Impact of security and redundancy measures

resources. Hence, we created four batches of 25 synthetic test cases each. Each test case has a random topology with 8 switches and 16 end-systems, 24 tasks, and multiple applications with random DAGs. Streams have a random RL between 1 and 3 and 30% probability to be considered security-critical. We also ran the same experiments with the auto test case from Table 3 to give an expectation for the overhead in a realistic scenario.

Each batch features either large (1000–1500 B) or small (1–250 B) streams and either large ( $\leq 10\%$  of period) or small ( $\leq 2\%$  of period) tasks. Each batch was run four times using the first feasible SA solution with different combinations of enabled/disabled security and redundancy requirements. Disabled security means that all streams are set to a security level of 0, while disabled redundancy means that all streams are set to a redundancy level of 1.

Table 4 shows the results. We always take the results for the no-security, no-redundancy run as a baseline and note the percentual increase in total cost, total bandwidth occupation percentage and total CPU utilisation percentage in the following rows. Bandwidth and CPU utilisation are measured as the mean of the utilisation over all links and ESs, respectively. Bandwidth utilisation for a specific link is the percentage of the hyperperiod in which streams are traversing this link. CPU utilisation for a specific ES is the percentage of the hyperperiod in which tasks are running.

As can be seen, the impact of adding security and redundancy differs significantly, depending on the size of initial streams and tasks. Note that an increase in overhead is expected with an increase in the number and difficulty of the security and redundancy requirements.

Adding redundancy has a negligible impact on cost and CPU utilisation but always has a significant impact on bandwidth. Adding security always has a significant impact on cost. This is because of the fundamental requirement of TESLA that sender and receiver tasks of secure streams lie in separate intervals, which will increase the end-to-end latency of the corresponding application. Therefore, the more consecutive secure streams exist in an application, the higher is the impact. However, our approach will always make sure that, if feasible, no application deadline is missed, despite the higher latency. The impact of adding security on bandwidth and CPU utilisation depends largely on the relative size of streams and WCET of tasks compared to the TESLA overhead. For example, the 16 B of overhead for a MAC is much more significant for a 100 B stream than for a 1000 B stream.

## 8.4 | Discussion

Our proposed SA implementation is able to determine good solutions in a reasonable time, even for large test cases. In addition, it can find feasible solutions (where all timing, safety, and redundancy requirements are satisfied) extremely quickly, within 10 s even for large test cases. This can be useful, for example, for evaluating several architectures in terms of their monetary costs and redundancy allowed by the physical

topology, prototyping or for rapid runtime reconfiguration in case of failures or changes in traffic patterns. Although CP can find optimal solutions, it does not scale for large test cases, and it is not flexible; that is, it will not report solutions that are not feasible. An advantage of SA is its ability to find return near-feasible solutions for those test cases that cannot be solved, that is, solutions with some infeasible applications or overlapping streams. SA can point out the offending apps/tasks and streams, which can give hints of where the configuration has to be improved to become feasible, for example, by increasing the redundancy in the physical topology or by changing the mapping of tasks to ESs.

## 9 | CONCLUSION

We addressed the combined TSN routing and scheduling problem for complex applications with redundancy and security requirements. We used TESLA, which is an efficient authentication protocol for use cases with multicast communication between low-power devices, with a modification to the protocol that makes it more lightweight, made possible by the real-time requirements of our network.

We developed two methods to solve the combined routing and scheduling problem: A Constraint Programming solution that can solve small and medium-sized test cases optimally and a solution that combines a Simulated Annealing metaheuristic and an ASAP list scheduling that can solve very large test cases. In the process, we formalised the constraints governing our problem and introduced novel ways to handle the complexities introduced by TESLA and redundancy while calculating correct solutions in the heuristic. Additionally, we developed an open-source tool for the reuse of our solutions and interactive visualisation of routes and schedules. Finally, we evaluated the impact of adding security and redundancy to existing applications and showed that the majority of overheads depend on the size of existing tasks and streams and thus ultimately on the requirements of the application area.

## DATA AVAILABILITY STATEMENT

Data that support the findings of this study are openly available on GitHub at <https://github.com/nreusch/TSNConf>.

## ORCID

Niklas Reusch  <https://orcid.org/0000-0002-2607-8389>

## REFERENCES

1. Gavriluț, V., Pop, P.: Traffic-type assignment for TSN-based mixed-criticality cyber-physical systems. *ACM Trans. Cyber-Phys. Syst.* 4(2), 1–27 (2020)
2. IEEE: Official Website of the 802.1 Time-Sensitive Networking Task Group. <http://www.ieee802.org/1/pages/tsn.html> (2016). Accessed 11 June 2021
3. Gavriluț, V., et al.: AVB-aware routing and scheduling of time-triggered traffic for TSN. *IEEE Access.* 6, 75229–75243 (2018)
4. Izosimov, V., et al. Design optimization of time- and cost-constrained fault-tolerant distributed embedded systems. In: *Proc. DATE* (2005)

5. Craciunas, S.S., et al.: Scheduling real-time communication in IEEE 802.1Qbv Time Sensitive Networks. In: Proc. RTNS. ACM (2016)
6. Gavriluț, V., et al.: Fault-tolerant topology and routing synthesis for IEEE time-sensitive networking. In: Proc. RTNS. ACM (2017)
7. Pereira, T., Barreto, L., Amaral, A.: Network and information security challenges within industry 4.0 paradigm. *Procedia Manuf.* 13, 1253–1260 (2017)
8. Studnia, I., et al.: Survey on security threats and protection mechanisms in embedded automotive networks. In: Proc. DSN (2013)
9. Perrig, A., et al.: Efficient and secure source authentication for multicast. In: Proc. NDSS, vol. 1 (2001)
10. Zhao, R., et al.: Security-aware scheduling for TTEthernet-based real-time automotive systems. *IEEE Access.* 7, 85971–85984 (2019)
11. Serna Oliver, R., Craciunas, S.S., Steiner, W.: IEEE 802.1Qbv gate control list synthesis using array theory encoding. In: Proc. RTAS. IEEE (2018)
12. Dürr, F., Nayak, N.G.: No-wait packet scheduling for IEEE time-sensitive networks (TSN). In: Proc. RTNS. ACM (2016)
13. Zhou, Y., et al.: ASIL-decomposition based routing and scheduling in safety-critical time-sensitive networking. In: Proc. RTAS (2021)
14. Houtan, B., et al.: Synthesising schedules to improve QoS of best-effort traffic in TSN networks. In: Proc. RTNS. ACM (2021)
15. Syed, A.A., et al.: Dynamic scheduling and routing for TSN based in-vehicle networks. In: Proc. ICC Workshops (2021)
16. Vlk, M., Hanzálek, Z., Tang, S.: Constraint programming approaches to joint routing and scheduling in time-sensitive networks. *Comput. Ind. Eng.* 157, 107317 (2021)
17. Vlk, M., et al.: Large-scale periodic scheduling in time-sensitive networks. *Comput. Oper. Res.* 137, 105512 (2022)
18. Wang, B., Hou, J.: Multicast routing and its QoS extension: problems, algorithms, and protocols. *IEEE Netw.* 14(1), 22–36 (2000)
19. Grammatikakis, M.D., et al.: Packet routing in fixed-connection networks: a survey. *J. Parallel Distr. Comput.* 54(2), 77–132 (1998)
20. A. Sheikh, et al.: Optimal design of virtual links in AFDX networks. *Real-Time Syst.* 49, 308–336 (2013)
21. D. Tămaș-Selicean, et al.: Design optimization of TTEthernet-based distributed real-time systems. *Real-Time Syst.* 51(1), 1–35 (2015)
22. Pham, Q.D., Deville, Y.: Solving the quorumcast routing problem by constraint programming. *Constraints.* 17(4), 409–431 (2012)
23. Ojewale M.A., Yomsi P.M.: Routing heuristics for load-balanced transmission in TSN-based networks. *SIGBED Rev.* 16(4) 20–25 (2020)
24. Laursen S.M., Pop P., Steiner W.: Routing optimization of AVB streams in TSN networks. *SIGBED Rev.* 13(4) 43–48 (2016)
25. Nayak, N.G., Dürr, F., Rothermel, K.: Routing algorithms for IEEE 802.1Qbv networks. *SIGBED Rev.* 15(3), 13–18 (2018)
26. Pahlevan, M., Tabassam, N., Obermaisser, R.: Heuristic list scheduler for time triggered traffic in time sensitive networks. *SIGBED Rev.* 16(1), 15–20 (2019)
27. Mahfouzi, R., et al.: Security-aware routing and scheduling for control applications on Ethernet TSN networks. *ACM Trans. Des. Autom. Electron. Syst.* 25(1), 1–26 (2019)
28. Huang, K., et al.: Reliability-aware multipath routing of time-triggered traffic in time-sensitive networks. *Electronics.* 10(2), 125 (2021)
29. Atallah, A.A., Hamad, G.B., Mohamed, O.A.: Routing and scheduling of time-triggered traffic in time-sensitive networks. *IEEE Trans. Ind. Inf.* 16(7), 4525–4534 (2020)
30. Reusch, N., Pop, P., Craciunas, S.S.: Work-In-Progress: safe and secure configuration synthesis for TSN using constraint programming. In: Proc. RTSS, pp. 387–390 (2020)
31. Issuing Committee: As-2d2 Deterministic Ethernet and Unified Networking, “SAE AS6802 Time-Triggered Ethernet”. <http://standards.sae.org/as6802/> (2011). Accessed 11 June 2021
32. W. Steiner, et al.: TTEthernet: time-triggered Ethernet. In: Obermaisser, R. (ed) Time-Triggered Communication. CRC Press (2011)
33. Prytz, G.: A performance analysis of EtherCAT and PROFINET IRT. In: Proc. ETFA. IEEE Computer Society (2008)
34. Seol, Y., et al.: Timely survey of time-sensitive networking: past and future directions. *IEEE Access.* 9, 142506–142527 (2021)
35. IEEE: 802.1AS-Rev – Timing and Synchronization for Time-Sensitive Applications. <http://www.ieee802.org/1/pages/802.1AS-rev.html> (2016). Accessed 11 June 2021
36. IEEE: 802.1Qbv – Enhancements for Scheduled Traffic. [https://standards.ieee.org/standard/802\\_1Qbv-2015.html](https://standards.ieee.org/standard/802_1Qbv-2015.html). Accessed 11 June 2021
37. IEEE: 802.1CB – Frame Replication and Elimination for reliability. [https://standards.ieee.org/standard/802\\_1CB-2017.html](https://standards.ieee.org/standard/802_1CB-2017.html) (2017). Accessed 11 June 2021
38. IEEE: 802.1Qbu – Frame Preemption. <http://www.ieee802.org/1/pages/802.1bu.html> (2016). Accessed 11 June 2021
39. IEEE: 802.1Qci – Per-Stream Filtering and Policing. [https://standards.ieee.org/standard/802\\_1Qci-2017.html](https://standards.ieee.org/standard/802_1Qci-2017.html) (2017). Accessed 11 June 2021
40. Pop, P., et al.: Design optimization of cyber-physical distributed systems using IEEE time-sensitive networks (TSN). *IET Cyber-Phys. Syst.: Theory Appl.* 1(1), 86–94 (2016)
41. Perrig, A., et al.: Timed efficient stream loss-tolerant authentication (TESLA): multicast source authentication transform introduction. Internet Requests for Comments, RFC Editor, RFC 4082 (2005)
42. Perrig, A., et al.: The TESLA Broadcast Authentication Protocol, pp. 2002. RSA CRYPTOBYTES (2002)
43. Falk, J., Dürr, F., Rothermel, K.: Exploring practical limitations of joint routing and scheduling for TSN with ILP. In: Proc. RTCSA, pp. 136–146 (2018)
44. Rossi, F., Van Beek, P., Walsh, T.: Handbook of Constraint Programming. Elsevier (2006)
45. Kirkpatrick, S., Gelatt, C.D., Jr., Vecchi, M.P.: Optimization by simulated annealing. *Science.* 220, 671–680 (1983)
46. Burke, E.K., Kendall, G.: Search Methodologies. Springer (2005)
47. Sinnen, O.: Fundamental Heuristics, pp. 108–144. John Wiley & Sons, Ltd (2007). ch. 5
48. Raagaard, M.L., Pop, P.: Optimization Algorithms for the Scheduling of IEEE 802.1 Time-Sensitive Networking (TSN). DTU Compute, Technical University of Denmark, Tech. Rep. (2017)
49. CP-SAT Solver Guide. [Online]. Available: [http://developers.google.com/optimization/cp/cp\\_solver](http://developers.google.com/optimization/cp/cp_solver)
50. Hagberg, A.A., Schult, D.A., Swart, P.J.: Exploring network structure, dynamics, and function using networkx. In: Proc. SciPy (2008)
51. Kandasamy, N., Hayes, J.P., Murray, B.T.: Dependable communication synthesis for distributed embedded systems. *Reliab. Eng. Syst. Saf.* 89(1), 81–92 (2005)
52. Cordeiro, D., et al.: Random graph generation for scheduling simulations. In: Proc. SIMUTools. ICST (2010)
53. Hutter, F., et al.: ParamLLS: an automatic algorithm configuration framework. *J. Artif. Intell. Res.* 36, 267–306 (2009)

**How to cite this article:** Reusch, N., Craciunas, S.S., Pop, P.: Dependability-aware routing and scheduling for Time-Sensitive Networking. *IET Cyber-Phys. Syst., Theory Appl.* 7(3), 124–146 (2022). <https://doi.org/10.1049/cps2.12030>

## APPENDIX

### A | Routing constraint formulation for forbidden overlap

To achieve a constraint formulation in which overlap of redundant streams is possible, the following steps need to be carried out:

Replace (RC2):

$$cost(s_n) = length\_cost(s_n) + 100 * overlap\_cost(s_n) \quad (RC2)$$

Introduce the following:

$$length\_cost(s_n) = \sum_{n \in \mathcal{N}\{s_n, t_s, e\}} (x(s_n, n) \neq nil) \quad (RC3)$$

$$overlap\_cost(s_n) = \sum_{n \in \mathcal{N}\{s_n, t_s, e\}} \sum_{m \in \mathcal{N} \setminus \{n\}} link\_cost(s_n, n, m) \quad (RC4)$$

$$link\_cost(s_n, n, m) = (xsum(s_n, n, m) - 1) * (x(s_n, n) == m) \quad (RC5)$$

Remove (R6). The overlap cost for a stream is dependent on how many redundant copies a stream overlaps with, and on how many links. In Equation (RC2) the total overlap cost is weighted with 100, but other values are also possible.

### B | Additional functions from metaheuristic formulation

#### 9.1 | Calculate Lower Bound

The function in Algorithm 10 determines the lower bound on the offset of a given block  $b$ . For a task or first stream instance, this is the maximum end-time of the blocks of the predecessors of the current entry  $n$  in the precedence graph  $p$  (lines 3–7). This

is the maximum end-time of all blocks from predecessor links for other stream instances on links (lines 8–12). Finally, for the stream instance on a receiver end-system, which models a MAC validation, the lower bound is the end-time of the corresponding key verification task, which is necessary to happen before a MAC can be validated (lines 13–17).

#### Algorithm 10 ASAP Heuristic – CalculateLower Bound

```

1 Function CalculateLowerBound( $n, b, P, \mathcal{R}$ )
2    $lb = 0;$ 
3   if  $b.prev == \emptyset$  then
4     /* If  $n$  is a task or the first stream instance */
5     foreach  $n_{prev} \in Predecessors(n, P)$  do
6        $b = LastBlock(n_{prev});$ 
7        $lb = \max(lb, b.o + Length(b));$ 
8     end
9   else if  $IsLink(b.l)$  then
10    /* If  $n$  is a stream and  $b.l$  is a link */
11    foreach  $l_{prev} \in PredecessorLinks(b.l, n, \mathcal{R})$  do
12       $b_{prev} = BlockOnLink(b.l, n);$ 
13       $lb = \max(lb, b_{prev}.o + Length(b_{prev}));$ 
14    end
15  else
16    /* If  $n$  is a stream and  $l$  is a receiver end-system */
17     $t_{key}^{verify} = GetKeyVerificationTask(n, l);$ 
18     $b_{key}^{verify} = GetBlockForEntry(t_{key}^{verify});$ 
19     $i = GetTESLAIIntervalForBlock(b_{key}^{verify});$ 
20     $lb = b_{key}^{verify}.o + i * b_{key}^{verify}.e.T + Length(b_{key}^{verify});$ 
21  end
22  return  $\max(lb, b.o);$ 

```

#### 9.2 | UpdateSchedule

The function in Algorithm 11 updates the schedule with all the blocks that were calculated for a given entry  $n$ . It iterates through all the links/nodes and the entry is scheduled on (line 3). It calculates all offsets and end-times across the

hyperperiod (lines 4–8) and proceeds to cut out the appropriate parts from the feasible regions for each existing period in the network (lines 9–20).

---

### Algorithm 11 ASAP Heuristic – UpdateSchedule

---

```

1 Function UpdateSchedule(n)
2   L = GetLinks(n);
3   foreach l ∈ L do
4     for i = 0 to  $\frac{H}{n \cdot T}$  do
5       offsets[i] = b.o + i * b.e.T;
6       endtimes[i] = b.o + i * b.e.T + Length(b);
7       i = i + 1;
8     end
9     /* Block queues/end-systems */
10    foreach T ∈ Periods do
11      for i = 0 to len(offsets)-1 do
12        o = offset[i];
13        e = endtimes[i];
14        if e%T < o%T then
15          /* Handle wrap around period
16           border */
17          CutFromFeasibleRegion(T, 1, o%T,
18                                T);
19          CutFromFeasibleRegion(T, 1, 0, e%T);
20        else
21          CutFromFeasibleRegion(T, 1, o%T,
22                                e%T);
23        end
24      end
25    end
26  end

```

---