Design and Verification Methodology for Secure and Performant Time-Sensitive Networks in Embedded Applications

Directrice de thèse : Ahlem Mifdaoui
Contact : ahlem.mifdaoui@isae-supaero.fr
Home page: http://personnel.isae.fr/ahlem-mifdaoui/
Co- encadrant de these: Marina Dehez Clementi
Contact: Marina.DEHEZ-CLEMENTI@isae-supaero.fr

Context and Objectives

Safety-critical embedded applications such as in aerospace and automotive require deterministic guarantees on the end-to-end latency of each flow and high levels of safety with zero congestion loss. Time-sensitive networking (TSN) standards [1] are considered as an appealing solution to provide such services while bringing wider homogeneity and standardization in embedded networks. These standards extend existing Ethernet protocols with real-time capabilities relying on a set of scheduling and redundancy mechanisms. The former aim to guarantee latency bounds whereas the later to reduce the probability of end-to-end losses. Furthermore, TSN standards offer management and configuration mechanisms that open the system to external communication and improve its reconfigurability level. However, these extended capabilities increase at the same time the attack surface of safety-critical functions and facilitate cybersecurity attacks leading to hazardous consequences for embedded systems and users, e.g., passengers. Therefore, in addition to performance and safety, security has to be considered during the development of the next generation of embedded communications technologies such TSN standards.

Although several works discuss the open issues of TSN mechanisms when focusing on one specific requirement like performance [3-5], safety [6] or security [7], there is no comprehensive work addressing the trade-offs between various requirements and/ or the effect of one requirement on the others.
While safety is usually the first objective when deploying new security mechanisms, these mechanisms may also impact the performance of the system, e.g., by introducing extra computation latency and/or extra communication overheads, and thus compromise in turn safety. Hence, the main objective of this thesis is to tackle the security and performance aspects (and their inter-relation) within first designing steps of of embedded systems using TSN standards for networking, to guarantee the most appropriate design under stringent requirements of security, performance and safety.

Main steps

1. **Analysis of the TSN standards vs security requirements**: starting from the security requirements of the considered embedded applications and case studies specified by the industrial partners, lead an extensive risk analysis of TSN standards, and particularly scheduling and redundancy mechanisms, to explore potential security issues and threats as well as to assess their impact on safety and probability of occurrence. There exist a variety of Threat Analysis and Risk Assessment methodologies (e.g., STPA-Sec [8], STRIDE, CORAS, HAZOP); some have already been applied to the analysis of cyber physical systems [9], but none is specific to TSN. Thus, a preliminary effort towards threat modelling in the context of TSN must be made. Then, when vulnerabilities with high impact on safety are identified, they have to be corrected

using mitigation techniques and countermeasures. These techniques have to be defined following a qualitative analysis to select the most suited ones to the considered application.

2. **Modeling and Analysis of the effect of security mechanisms on performance metrics**: for safety-critical embedded applications, real-time constraints must be guaranteed. In addition, several countermeasures may solve a security issue. The use of security mechanisms will introduce several communication overheads and this may impact the end-to-end latencies, the memory occupation and the bandwidth utilization. Therefore, an appropriate proof of determinism should be considered. One of the methods widely used to validate these constraints is the Network Calculus [2]. Hence, we need first to define Network Calculus-based models for the selected security mechanisms and then to derive performance analyses of the global communication architecture. This quantitative analysis will enable the selection of the most suitable security mechanisms offering the best trade-offs between both aspects, i.e., security and performance, and take the most appropriate decision concerning the network design.

3. **Validation on industrial case studies**: after the qualitative and quantitative analyses of the selected security and TSN mechanisms, performance validation on industrial case studies is necessary to consolidate the choices of the considered mechanisms.

Key words
TSN, embedded applications, performance analysis, security, Network Calculus

Informations & Profile:
- Possibility to start with an internship from March 2024
- PHD thesis from October 2024 within an industrial project
- Profile: Master thesis or engineer diploma in computer science/ networks/ embedded systems with good skills in security

References
[1] IEEE. (2018). IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks (IEEE Std 802.1Q-2018). IEEE. https://ieeexplore.ieee.org/document/8293544
[2] Le Boudec, J.-Y., & Thiran, P. (2001). Network Calculus: A Theory of Deterministic Queuing Systems for the Internet. Lecture Notes in Computer Science. Springer-Verlag. https://www.springer.com/us/book/9783540421849
[3] Thomas, L., Le Boudec, J.-Y., & Mifdaoui, A. (2019). On Cyclic Dependencies and Regulators in Time-Sensitive Networks. In 2019 IEEE Real-Time Systems Symposium (RTSS) (pp. 299–311). IEEE. https://ieeexplore.ieee.org/document/9048517
[4] Thomas, L., & Le Boudec, J.-Y. (2020). On Time Synchronization Issues in Time-Sensitive Networks with Regulators and Nonideal Clocks. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 4, 27:1–27:41. https://doi.org/10.1145/3392145
[5] Zhao, L., Pop, P., & Steinhorst, S. (2021). Quantitative Performance Comparison of Various Traffic Shapers in Time-Sensitive Networking. arXiv:2103.13424. http://arxiv.org/abs/2103.13424
[6] Thomas, L., Mifdaoui, A., & Le Boudec, J.-Y. (2022). Worst-Case Delay Bounds in Time-Sensitive Networks With Packet Replication and Elimination. IEEE/ACM Transactions on Networking, 30(6), 2701–2715. https://doi.org/10.1109/TNET.2022.3180763
[7] Ergenç, D., Brülhart, C., Neumann, J., Krüger, L., & Fischer, M. (2021). On the Security of IEEE 802.1 Time-Sensitive Networking. In 2021 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1–6). IEEE.
[8] Young, W., & Porada, R. (2017). System-theoretic process analysis for security (STPA-SEC): Cyber security and STPA. In 2017 STAMP Conference.
[9] Sahay, R., Estay, D. S., Meng, W., Jensen, C. D., & Barfod, M. B. (2023). A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS. Computers & Security, 128, 103179.