Offre de stage master

Configurations Vulnérables dans les Réseaux Sensibles à la Latence : Identification et caractérisation

Contexte et problématique

L'architecture TSN (Time Sensitive Networking) désigne un ensemble de standards IEEE conçus dans l'objectif de faire évoluer le réseau Ethernet d'aujourd'hui vers un réseau supportant les communications déterministes et temps-réel de certaines applications [1] : automatisation industrielle, automobile, avioniques, etc. Afin de satisfaire les exigences très strictes de ces applications en matière de qualité de service (délai, gigue, perte de paquets, etc.), l'organisme de standardisation IEEE a défini une suite de standards [2] permettant de gérer principalement : la synchronisation temporelle entre les équipements TSN (Time Synchronization), la planification des trafics de données (Scheduling), l'orchestration et la réservation de ressources (Orchestration and Reservation) ainsi que le filtrage et la redondance (Policing and Redundancy).

La sécurité de certaines fonctionnalités et communications des standards TSN a été intégrée par conception, notamment par le biais d'un composant appelé *Per Stream Filtering and Policing* (PSFP) qui a pour objectif d'assurer l'isolation des flux afin de garantir leur exigence temporelle tout au long du transit sur le réseau. Si ce composant offre les moyens opérationnels pour assurer l'isolation des flux et leur respect des contraintes de latence exprimés, sa configuration est un problème difficile [4] du fait de la complexité et la diversité des éléments à configurer (filtrage, synchronisation de portes, configuration de crédits, etc.) qu'un administrateur peut résoudre par des simplifications de configuration ou simplement en passant outre des configurations erronées qui ne sont pas le reflet de l'usage actuel du réseau déployé. Par ce biais, la contrainte de temps peut devenir un vecteur d'attaque qu'un attaquant peut exploiter en retardant par exemple la livraison de paquets causant ainsi des dégâts considérables sur l'application visée [3].

État de l'art

De récents travaux de recherche ont pour objectif d'automatiser la configuration des composant d'un réseau TSN [5, 6]. Le travail décrit dans [6] montre la faisabilité d'une telle configuration dans un réseau TSN simulé (NeSTiNg [7], basé sur OMNeT++) et évalue le délai de bout-en-bout des différents flux critiques considérés. Comme ce délai présente des variations importantes entre les différents flux (de 24 à 1888 µs), l'auto-configuration, ou la configuration d'une manière générale, d'un réseau TSN peut conduire à des résultats différents de ceux qui sont attendus, voire même à des situations défaillantes avec des failles de sécurité. Par exemple, la non prise en compte de la granularité d'un flux peut conduire à l'admission de certains autres flux non autorisés et à la suppression, par la suite, de paquets du flux légitime. Ainsi, la sécurité des réseaux TSN est un aspect important qu'il faut prendre en compte. Dans [8], ceci a été pris en considération lors de la configuration du routage et de la planification dans un réseau TSN afin d'éviter les interférences malicieuses d'autres flux tout en garantissant la qualité de service nécessaire aux flux critiques légitimes.

Objectif et travail demandé

L'objectif de ce stage est de simuler le fonctionnement d'un réseau TSN configuré grâce à un ou plusieurs algorithmes d'auto-configuration afin d'identifier des situations « défaillantes » qui peuvent être exploitées par un attaquant [9]. Ceci passe par l'injection de flux légitimes mais aussi de flux illégitimes pour évaluer le comportement du réseau TSN dans le cadre de chaque configuration. L'identification de scénarios menant à de tels dysfonctionnements permettra : (i) d'identifier les failles de sécurité liées à la configuration des éléments d'un nœud TSN et (ii) de définir des mécanismes pour la détection et la correction de ces failles.
Ainsi, le travail demandé est organisé comme suit :

1. État de l'art sur les réseaux TSN et la configuration détaillée d'un nœud TSN ;
2. ***S***imulation d'un réseau TSN auto-configuré en utilisant différents algorithmes/approches ;
3. Identification de situations défaillantes où des paquets d'un flux critique légitime subissent une suppression ou un délai hors-norme ;
4. Définir des mesures de protection comme la correction automatique de la configuration d'un élément TSN et évaluation de l'efficacité des mesures définies.

Compétences nécessaires

Ce stage vise des candidatures de niveau M2 ou équivalent, comme la dernière année d'école d'ingénieur. Des compétences générales en système, réseaux et sécurité sont attendues. Des connaissances sur les architectures en réseaux de dernière génération seront appréciées.

Conditions du stage

Le stage se déroule au sein l'équipe SOTERN de l'IRISA dans les locaux de Lannion. Le stagiaire aura accès à la plateforme du laboratoire et aux ressources nécessaires pour le travail (poste de travail, ressources bibliographiques, etc.). La rémunération de stage se situe autour de 530€ par mois.

Références

[1] L. Lo Bello and W. Steiner, "A Perspective on IEEE Time-Sensitive Networking for Industrial Communication and Automation Systems", Procedeeings of the IEEE, vol. 107, no. 6, June 2019, doi: 10.1109/JPROC.2019.2905334.
[2] IEE802.1 Standards, IEEE 802.1 Working Group, https://1.ieee802.org
[3] D. Ergenç, C. Brülhart, J. Neumann, L. Krüger and M. Fischer, "On the Security of IEEE 802.1 Time-Sensitive Networking," *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICCWorkshops50388.2021.9473542.
[4] Lejla Smajlovic Dalila Alibegovic. « Time Sensitive Network (TSN) configurations on network performance in real-time communication. 2022. url : https : //www.diva-portal.org/smash/get/diva2:1667807/FULLTEXT01.pdf.
[5] M. Gutiérrez, A. Ademaj, W. Steiner, R. Dobrin and S. Punnekkat, "Self-configuration of IEEE 802.1 TSN networks," *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Limassol, Cyprus, 2017, pp. 1-8, doi: 10.1109/ETFA.2017.8247597.
|6] B. Houtan, A. Bergström, M. Ashjaei, M. Daneshtalab, M. Sjödin and S. Mubeen, "An Automated Configuration Framework for TSN Networks," *2021 22nd IEEE International Conference on Industrial Technology (ICIT)*, Valencia, Spain, 2021, pp. 771-778, doi: 10.1109/ICIT46573.2021.9453628.
[7] D. Hellmanns and J. Falk. (2020) Nesting - network simulator for timesensitive networking. [Online]. Available: https://gitlab.com/ipvs/nest
[8] Mahfouzi R, Aminifar A, Samii S, Eles P, Peng Z. Security-aware routing and scheduling for control applications on Ethernet TSN networks. ACM Transactions on Design Automation of Electronic Systems (TODAES), nov. 2019, pp.1-26.
[9] Craciunas SS, Oliver RS, Chmel´ık M, Steiner W. Scheduling real-time communication in IEEE 802.1 Qbv time sensitive networks. In Proceedings of the 24th International Conference on Real- Time Networks and Systems, oct. 2016, pp. 183-192.

Encadrants

Mohamed-Aymen CHALOUF (mohamed-aymen.chalouf@irisa.fr)
SOTERN, IRISA, Lannion

Guillaume DOYEN (guillaume.doyen@imt-atlantique.fr)
SOTERN, IRISA, Rennes

David ESPES (david.espes@univ-brest.fr)
IRIS, LABSTICC, Brest