PFE 1

Dr. Anwer kalghoum - anwer.kalghoum@gmail.com

January 2026

1 Proposition PFE 1 : Protection des réseaux IoT basée sur le méta-apprentissage

1.1 Résumé (Proposition PFE)

Les réseaux IoT sont caractérisés par leur hétérogénéité, leurs ressources limitées et leur forte exposition aux cyberattaques. Les solutions de sécurité traditionnelles, basées sur des modèles d'apprentissage statiques, peinent à s'adapter aux nouveaux types d'attaques et aux environnements dynamiques. Ce projet propose une approche innovante basée sur le *méta-apprentissage* (Meta-Learning) afin de concevoir un système de détection d'intrusions capable d'apprendre rapidement à partir d'un nombre réduit d'exemples et de s'adapter efficacement à de nouvelles attaques, y compris les attaques zero-day. Le modèle sera conçu pour être léger, rapide et adapté aux contraintes des dispositifs IoT.

1.2 Objectifs du projet

- Étudier les vulnérabilités et menaces spécifiques aux réseaux IoT.
- Concevoir un système IDS basé sur le méta-apprentissage.
- Permettre une adaptation rapide du modèle à de nouvelles attaques.
- Comparer les performances avec des approches classiques de Machine Learning et Deep Learning.
- Optimiser la consommation des ressources (CPU, mémoire, énergie).

1.3 Cahier des charges

- Collecte et prétraitement de datasets IoT (ex. : Bot-IoT, IoT-23).
- Implémentation de modèles de méta-apprentissage (MAML, Reptile).
- Déploiement d'un prototype IDS simulé ou réel.

- Évaluation selon plusieurs métriques : précision, rappel, F1-score, temps d'adaptation.
- Génération de rapports et visualisations des résultats.

References

[1] Kaliski, R. (2025). *Meta-learning for cyber-attack detection in IoT networks*. In *Advanced Machine Learning for Cyber-Attack Detection in IoT Networks*, Elsevier, pp. 143–164.

[2] Bahranifard, Z. and Ghaffari, S. (2025). *A Survey of Meta-learning: Paradigms, Applications, and Challenges*. Available at SSRN.

[3] Wu, Y. et al. (2024). *MASiNet: Network Intrusion Detection for IoT Security Based on Meta-Learning Framework*. IEEE Internet of Things Journal, vol. 11, no. 14, pp. 25136–25146.

[4] Finn, C., Abbeel, P., & Levine, S. (2017). *Model-Agnostic Meta-Learning for Fast Adaptation of Deep Networks*. ICML.

[5] Meidan, Y. et al. (2018). *N-BaIoT: Network-based Detection of IoT Botnet Attacks*. IEEE Pervasive Computing.

[6] Shone, N. et al. (2018). *A Deep Learning Approach to Network Intrusion Detection*. IEEE TETCI.