الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي ٠8 ماي 1945 ٠ بسيدي بلعباس
Higher School of Computer Science
-08 May 1945- Sidi Bel Abbès

CESI LINEACT

Graduation Thesis

Submitted to obtain the **Engineering degree**
Field of Study : **Computer Science**
Specialization: **Computer Systems Engineering (ISI)**

Topic

Toward Secure IoT-Based Smart Systems: A Focus on Security in IoT Network Protocols

---

Presented by: **Mohamed Chakib OUZANE**
Internship conducted at **CESI LINEACT Research Lab**, Aix-en-Provence, France

Submission Date: **23.09.2025**
Presented to the jury panel consisting of:

President	Mr	BENSENANE Hamdane	M.C.A.	ESI-SBA, Algérie.
Examiner	Mr	BENDAOUD Fayssal	M.C.A.	ESI-SBA, Algeria.
Supervisor	Mr	RAHMOUN Abdelatif	Prof.	ESI-SBA, Algeria.
Co-Supervisor	Mr	BOUDOUAIA Mohammed Amine	E.C.	CESI, France.

Academic Year : 2024/2025

Abstract

Nowadays, smart systems are experiencing a global popularity, driven by a rapid advancement of information technology and the integration of Internet of Things (IoT) devices. These technologies transform how we interact with indoor and outdoor environments by enabling automation, optimizing energy efficiency, and enhancing environmental monitoring. However, as IoT-enabled systems scale up in smart cities, they encounter significant security challenges. These challenges are directly tied to the underlying network protocols and their vulnerabilities, particularly in Low-power and Lossy Networks (LLNs). Addressing these challenges requires innovative approaches to strengthen the security of network protocols in IoT systems, especially those operating within LLNs, where resource constraints and network instability further complicate the application of security measures. Artificial Intelligence (AI) and Machine Learning (ML) are increasingly being utilized to detect and mitigate security threats in real-time by analyzing network behavior and identifying anomalies. However, traditional ML approaches often require centralized data collection, which can introduce privacy risks and scalability issues. To overcome this, Federated Learning (FL) offers a decentralized alternative, enabling IoT devices within LLNs to collaboratively improve security models without exposing sensitive data. This thesis contributes by proposing and analyzing two novel DIS-based attacks, TIDE and DRIFT, in simulated RPL networks, and by designing a federated learning–based detection and mitigation framework. The proposed solution enhances the security and resilience of RPL-based IoT networks while addressing privacy, scalability, and resource efficiency concerns.

Keywords — Internet of Things (IoT), Routing Protocol for Low-Power and Lossy Networks (RPL), Security, Attacks, Comprehensive Review, Machine Learning

الملخص

في الوقت الحاضر، تشهد الأنظمة الذكية انتشارًا عالميًا متزايدًا، مدفوعًا بالتطور السريع في تكنولوجيا المعلومات واندماج أجهزة إنترنت الأشياء (IoT). تعمل هذه التقنيات على تغيير طريقة تفاعلنا مع البيئات الداخلية والخارجية من خلال تمكين الأتمتة، وتحسين كفاءة استهلاك الطاقة، وتعزيز مراقبة البيئة. ومع ذلك، مع توسع أنظمة إنترنت الأشياء في المدن الذكية، فإنها تواجه تحديات أمنية كبيرة. ترتبط هذه التحديات بشكل مباشر ببروتوكولات الشبكات الأساسية ونقاط ضعفها، لا سيما في الشبكات منخفضة الطاقة وعالية الفقدان (LLNs). لمواجهة هذه التحديات، هناك حاجة إلى نهج مبتكرة لتعزيز أمان بروتوكولات الشبكات في أنظمة إنترنت الأشياء، خاصة التي تعمل ضمن الشبكات منخفضة الطاقة وعالية الفقدان (LLNs)، حيث تؤدي قيود الموارد وعدم استقرار الشبكة إلى تعقيد تدابير الأمان. يتم استخدام الذكاء الاصطناعي (AI) والتعلم الآلي (ML) بشكل متزايد للكشف عن التهديدات الأمنية والتخفيف من حدتها، وذلك من خلال تحليل سلوك الشبكة وتحديد الأنماط الشاذة. ومع ذلك، غالبًا ما تتطلب أساليب التعلم الآلي التقليدية جمع البيانات مركزيًا، مما قد يؤدي إلى مخاطر تتعلق بالخصوصية ومشكلات في قابلية التوسع. لمعالجة هذه المشكلة، يوفر التعلم الفيدرالي (FL) بديلاً لامركزيًا، مما يتيح لأجهزة إنترنت الأشياء ضمن الشبكات منخفضة الطاقة وعالية الفقدان تحسين نماذج الأمان بشكل تعاوني دون الحاجة لكشف البيانات الحساسة. تُساهم هذه الأطروحة من خلال اقتراح وتحليل هجومين جديدين TIDE و DRIFT وكذلك من خلال تصميم إطار للكشف والتخفيف يعتمد على التعلم الفيدرالي. يعمل الحل المقترح على تعزيز أمان ومرونة شبكات إنترنت الأشياء المعتمدة على RPL مع معالجة القضايا المتعلقة بالخصوصية، وقابلية التوسع وكفاءة الموارد.

الكلمات الدالة:
إنترنت الأشياء، بروتوكول التوجيه للشبكات منخفضة الطاقة وعالية الفقدان RPL، رسائل التحكم في RPL، مراجعة شاملة، التعلم الآلي، التعلم الفيدرالي، الأمن السيبراني

Résumé

De nos jours, les systèmes intelligents connaissent un essor mondial, porté par les avancées rapides des technologies de l'information et l'intégration des dispositifs de l'Internet des objets (IoT). Ces technologies transforment notre interaction avec les environnements intérieurs et extérieurs en permettant l'automatisation, en optimisant l'efficacité énergétique et en améliorant la surveillance environnementale. Cependant, à mesure que les systèmes basés sur l'IoT se déploient à grande échelle dans les villes intelligentes, ils rencontrent d'importants défis en matière de sécurité. Ces défis sont directement liés aux protocoles réseau sous-jacents et à leurs vulnérabilités, en particulier dans les réseaux à faible consommation et à pertes (LLNs). Relever ces défis nécessite des approches innovantes pour renforcer la sécurité des protocoles réseau dans les systèmes IoT, en particulier ceux fonctionnant au sein des LLNs, où les contraintes de ressources et l'instabilité du réseau compliquent davantage l'application des mesures de sécurité. L'intelligence artificielle (IA) et l'apprentissage automatique (ML) sont de plus en plus utilisés pour détecter et atténuer les menaces de sécurité en temps réel en analysant le comportement du réseau et en identifiant les anomalies. Cependant, les approches traditionnelles du ML nécessitent souvent une collecte centralisée des données, ce qui peut entraîner des risques pour la confidentialité et des problèmes de mise à l'échelle. Pour pallier ces limitations, l'apprentissage fédéré (FL) propose une alternative décentralisée, permettant aux dispositifs IoT au sein des LLNs d'améliorer collaborativement les modèles de sécurité sans exposer de données sensibles. Cette thèse contribue en proposant et en analysant deux nouvelles attaques basées sur DIS, TIDE et DRIFT, dans des réseaux RPL simulés, et en concevant un cadre de détection et de mitigation basé sur l'apprentissage fédéré. La solution proposée améliore la sécurité et la résilience des réseaux IoT basés sur RPL, tout en répondant aux préoccupations liées à la confidentialité, à la scalabilité et à l'efficacité des ressources.

Mots Clés — Internet des objets, Protocole de routage pour les réseaux à faible consommation et à pertes, Messages de contrôle RPL, étude approfondie, Apprentissage automatique, Apprentissage fédéré, Sécurité