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 ٠08 ماي 1945 ٠ بسيدي بلعباس
Higher School of Computer Science
-08 May 1945- Sidi Bel Abbès

CESI LINEACT

Graduation Thesis

Submitted to obtain the **Master's 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 global popularity, driven by rapid advancements in IT and the widespread deployment of Internet of Things (IoT) devices. These technologies are transforming interactions with indoor and outdoor environments by enabling automation, optimizing energy efficiency, and enhancing environmental monitoring. In particular, Low-power and Lossy Networks (LLNs) form the backbone of many IoT deployments, facilitating communication between constrained devices. However, as these networks scale up, they face critical security challenges. These challenges are often rooted in the vulnerabilities of network protocols, with the Routing Protocol for Low-Power and Lossy Networks (RPL), widely used for routing in LLNs, being especially susceptible to various attacks.
Ensuring the security of RPL networks requires strategies that address both protocol-level weaknesses and network constraints. Lightweight & efficient security mechanisms are essential, given the limited computational and energy resources of IoT devices. This thesis investigates the security threats targeting RPL, analyzes their impact, and explores potential mitigation techniques to enhance the resilience of IoT networks. By understanding the interplay between IoT devices, network topology, and RPL, this work aims to contribute to the development of more secure IoT.

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

الملخص

في الوقت الحاضر، تشهد الأنظمة الذكية انتشارًا واسعًا على الصعيد العالمي، مدفوعة بالتقدم السريع في تكنولوجيا المعلومات والانتشار الواسع لأجهزة إنترنت الأشياء (IoT). تعمل هذه التقنيات على تغيير طريقة تفاعلنا مع البيئات من خلال تمكين الأتمتة، وتحسين كفاءة استهلاك الطاقة، وتعزيز مراقبة البيئة. تشكل الشبكات منخفضة الطاقة وعالية الفقدان (LLNs) العمود الفقري للعديد من تطبيقات إنترنت الأشياء ، حيث تسهل التواصل بين الأجهزة ذات الموارد المحدودة. ومع تزايد حجم هذه الشبكات، تواجه تحديات أمنية خطيرة. وغالبًا ما تنبع هذه التحديات من نقاط ضعف بروتوكولات الشبكة، خاصة بروتوكول التوجيه لشبكات منخفضة الطاقة وعالية الفقدان (RPL) الذي يُستخدم على نطاق واسع في توجيه البيانات داخل شبكات LLNs.

يتطلب ضمان أمان شبكات إنترنت الأشياء المعتمدة على بروتوكول RPL استراتيجيات تعالج كلًا من نقاط ضعف البروتوكول وقيود الشبكة. ومن الضروري وجود آليات أمان خفيفة وفعالة نظرًا لمحدودية القدرات الحسابية وموارد الطاقة في أجهزة إنترنت الأشياء. تبحث هذه الرسالة في التهديدات الأمنية التي تستهدف بروتوكول RPL وتحلل تأثيرها على الأداء، وتستكشف تقنيات التخفيف المحتملة لتعزيز متانة شبكات إنترنت الأشياء. ومن خلال فهم التفاعل بين أجهزة إنترنت الأشياء، وطوبولوجيا الشبكة، ونقاط ضعف بروتوكول RPL , يهدف هذا العمل إلى المساهمة في تطوير نشرات إنترنت الأشياء أكثر أمانًا وقوة.

الكلمات الدالة:
إنترنت الأشياء، بروتوكول التوجيه للشبكات منخفضة الطاقة وعالية الفقدان RPL، الأمن السيبراني، مراجعة شاملة

Résumé

De nos jours, les systèmes intelligents connaissent une popularité mondiale, portée par les avancées rapides des technologies de l'information et le déploiement massif des dispositifs de l'Internet des objets (IoT). Ces technologies transforment les interactions avec les environnements en permettant l'automatisation, en optimisant l'efficacité énergétique. En particulier, les réseaux basse consommation et à perte (LLNs) constituent la colonne vertébrale de nombreuses applications IoT, facilitant la communication entre dispositifs contraints. Cependant, à mesure que ces réseaux se développent, ils font face à des défis critiques en matière de sécurité. Ces défis découlent souvent des vulnérabilités des protocoles réseau, notamment le protocole RPL, largement utilisé pour le routage dans les LLNs, qui reste particulièrement vulnérable à divers types d'attaques.
Assurer la sécurité des réseaux IoT basés sur RPL nécessite des stratégies globales prenant en compte à la fois les faiblesses du protocole et les contraintes du réseau. Des mécanismes de sécurité légers et efficaces sont indispensables, compte tenu des ressources limitées en calcul et en énergie des dispositifs IoT. Cette thèse étudie les menaces pesant sur RPL, analyse leur impact, et explore les techniques possibles afin de renforcer la résilience des réseaux IoT. En comprenant l'interaction entre les dispositifs IoT, la topologie réseau et les vulnérabilités de RPL, ce travail vise à contribuer au développement de déploiements IoT plus sûrs et robustes.

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