PEOPLE'S DEMOCRATIC REPUBLIC of ALGERIA
Ministry of Higher Education and Scientific Research
Ferhat Abbas University of Sétif 1
Faculty of Sciences
Department of Computer Science



Theme

Strengthening Smart Irrigation System Against Network Attacks

Presented by:

MAHMOUDI Laldja & ABBACI Souad

As a requirement to aim for the degree of Master in networks and distributed systems

Supervised by : Dr. Chirihane Gherbi

2025 / 2026

Abstract

The integration of IoT technologies in smart irrigation systems has improved agricultural efficiency through real-time monitoring and automated water management, but exposes these systems to cyber threats such as DoS, DDoS, spoofing, and flooding attacks, which can disrupt irrigation operations and cause severe crop damage. To address this, we propose DeepIrri-IDS, a deep learning-based intrusion detection system deployed at the fog layer, that integrates SimPy- based irrigation simulation, cyber-attack injection using the Farm-Flows dataset, and SMOTE oversampling to handle class imbalance, evaluating four deep learning architectures: CNN, LSTM, FT-Transformer, and Mamba. Experimental results demonstrate that all models exceed 99% accuracy on the Farm-Flows dataset, with the LSTM model selected as the most suitable architecture for real-time deployment, achieving 99.39% accuracy and the fastest inference time of 27.97 μs per packet, offering the best balance between detection performance and computational efficiency in resource-constrained IoT environments, successfully blocking malicious traffic before it reaches the irrigation controller and maintaining stable and continuous system operation despite the presence of diverse cyberattacks.

Keywords: Smart Irrigation, Intrusion Detection, Deep Learning, Network Security, Internet of Things.

Résumé

L'intégration des technologies de l'Internet des Objets (IoT) dans les systèmes d'irrigation intelligents a conduit à l'émergence de systèmes permettant la surveillance en temps réel et la gestion automatisée de l'eau. Cependant, la connectivité croissante de ces systèmes les expose à des cybermenaces telles que les attaques DoS, DDoS, usurpation et inondation, ciblant les dispositifs IoT vulnérables et pouvant perturber les opérations d'irrigation et causer des dommages importants aux cultures. Pour répondre à ces enjeux, ce travail propose DeepIrri-IDS, un système de détection d'intrusion basé sur l'apprentissage profond, déployé au niveau de la couche fog, intégrant une simulation d'irrigation basée sur SimPy, une injection d'attaques cybernétiques à l'aide du dataset Farm-Flows, et la technique SMOTE pour gérer le déséquilibre des classes, en évaluant quatre architectures : CNN, LSTM, FT-Transformer et Mamba. Les résultats expérimentaux démontrent que tous les modèles dépassent 99% de précision, avec le modèle LSTM sélectionné comme l'architecture la plus adaptée au déploiement en temps réel, atteignant 99,39% de précision et le temps d'inférence le plus rapide de 27,97 μs par paquet. Ces contributions démontrent l'efficacité de l'apprentissage profond pour améliorer la cybersécurité dans les environnements d'irrigation intelligents basés sur l'IoT.

Mots-clés: Irrigation Intelligente, Détection d'Intrusion, LSTM, SMOTE, IoT.

ملخص

أدى دمج تقنيات إنترنت الأشياء IoT في أنظمة الري الذكية إلى ظهور أنظمة تتيح المراقبة في الوقت الحقيقي وإدارة المياه بشكل آلي. ومع ذلك، فإن الاتصال المتزايد لهذه الأنظمة يعرضها لتهديدات إلكترونية مثل هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزعة $DDoS$ والاختراق والفيضانات، التي تستهدف أجهزة إنترنت الأشياء الضعيفة وقد تعطل عمليات الري وتسبب أضراراً جسيمة للمحاصيل. ولمواجهة هذه التحديات، يقترح هذا العمل نظام $DeepIrri-IDS$ ، وهو نظام كشف عن التسلل يعتمد على التعلم العميق، يتم نشره على مستوى طبقة الضباب، ويدمج محاكاة نظام الري باستخدام $SimPy$ ، وحقن الهجمات السيبرانية بمساعدة مجموعة بيانات $Farm-Flows$ ، وتقنية $SMOTE$ لإدارة عدم توازن الفئات، مع تقييم أربع بنى: CNN و $LSTM$ و $FT-Transformer$ و $Mamba$.
أظهرت النتائج التجريبية أن جميع النماذج تتجاوز دقة 99% ، مع اختيار نموذج $LSTM$ باعتباره البنية الأكثر ملاءمة للنشر في الوقت الفعلي، حيث حقق دقة 99.39% وأسرع وقت استدلال بلغ 27.97 ميكروثانية لكل حزمة.
تُبرز هذه النتائج فعالية التعلم العميق في تحسين الأمن السيبراني في بيئات الري الذكي القائمة على إنترنت الأشياء.

الكلمات المفتاحية: الري الذكي، نظام كشف التسلل، التعلم العميق، الهجمات الإلكترونية.

Table of contents

Abstract 1

Résumé 2

Table of contents I

List of figures III

List of tables IV

General Introduction 2

1 State of the Art 3

1.1 Introduction . . . 3

1.2 Internet of Things (IoT) in Smart Agriculture . . . 3

1.3 IoT Architecture for Smart Irrigation . . . 4

1.3.1 Perception Layer . . . 5

1.3.2 Network Layer . . . 5

1.3.3 Storage and Data Analysis Layer . . . 5

1.3.4 Application Layer . . . 6

1.4 IoT Communication Protocols in Smart Irrigation . . . 6

1.5 Network Threats and Attacks in IoT-Based System . . . 7

1.5.1 DoS Attacks . . . 8

1.5.2 DDoS Attacks . . . 9

1.5.3 Man-in-the-Middle Attacks . . . 9

1.5.4 False Data Injection (FDI) Attacks . . . 10

1.5.5 Spoofing and Replay Attacks . . . 10

1.5.6 Eavesdropping . . . 10
1.6 Security Mechanisms for IoT Networks . . . 11
1.6.1 Cryptographie . . . 11
1.6.2 Authentification . . . 11
1.6.3 Intrusion Detection System (IDS) . . . 12
1.6.4 Blockchain . . . 12
1.6.5 Artificial Intelligence (AI) . . . 12
1.7 Advantages and limitations of security solutions in IoT . . . 13
1.8 Conclusion . . . 14

2 Related Review **15**
2.1 Introduction . . . 15
2.2 Intrusion Detection Systems (IDS) for IoT Networks . . . 15
2.2.1 Definition of IDS . . . 15
2.2.2 Types of IDS . . . 15
2.2.3 Detection Techniques . . . 16
2.2.4 Advantages and Limitations of IDS for IoT . . . 17
2.3 Deep Learning for Attack Detection in IoT . . . 17
2.3.1 Deep Learning Techniques for Intrusion Detection . . . 17
2.3.2 DL Models for Intrusion Detection . . . 18
2.4 Related Work . . . 19
2.4.1 Smart Irrigation Security Using IOTA Distributed Ledger . . . 19
2.4.2 Digital Twin based What-if Simulation of Security Attacks in Smart Irrigation Systems (Ramesh et al., 2024) . . . 20
2.4.3 Intrusion Detection Using Machine Learning for Risk Mitigation in IoT-Enabled Smart Irrigation . . . 21
2.4.4 Smart Irrigation with Intrusion Detection Using Adler32 Hashing 22
2.5 Conclusion . . . 24

3 Deep Learning for Irrigation Intrusion Detection System **26**
3.1 Introduction . . . 26
3.2 Proposed approach . . . 27

3.2.1 DeepIrri-IDS (Deep Learning for Irrigation Intrusion Detection System . . . 27
3.3 Conclusion . . . 40

4 Discussion of Results **41**
4.1 Introduction . . . 41
4.2 Tools Description . . . 41
4.2.1 Hardware Environment . . . 45
4.3 Datasets used . . . 46
4.4 Evaluation Metrics . . . 47
4.4.1 Confusion Matrix . . . 47
4.5 Results and discussion . . . 50
4.5.1 Irrigation System Behavior Analysis . . . 50
4.5.2 Deep Learning Models Performance Evaluation . . . 51
4.5.2.1 CNN Model . . . 51
4.5.2.2 LSTM Model . . . 55
4.5.2.3 FT-Transformer Model . . . 57
4.5.2.4 Mamba Model . . . 61
4.5.3 Comparative Analysis of Deep Learning Models . . . 64
4.5.4 LSTM-Based IDS Protection Against Network Attacks . . . 65
4.6 Conclusion . . . 66

General Conclusion **68**

Bibliography **68**