جامعة الموصل
كلية التربية للعلوم الصرفة

طريقة تعلم فيدرالية لكشف التطفل في الشبكة باستخدام تصنيف العملاء الموثوقين

حذيفة انور محمد حسن

رسالة ماجستير

قسم علوم الحاسوب

بإشراف

الأستاذ المساعد

الدكتور أوس خزعل علي

١٤٤٧هـ ٢٠٢٥ م

الملخص

أدى التوسع الهائل في الفضاء السيبراني والاعتماد المتزايد على المعاملات الرقمية وانتشار الأجهزة المتصلة بالشبكات إلى تصاعد غير مسبوق في حجم وتعقيد التهديدات السيبرانية. ولمواجهة هذه التهديدات، برزت أنظمة كشف التطفل (IDS) كأحد أهم خطوط الدفاع لحماية البيانات والبنى التحتية الرقمية. ومع ذلك، تواجه الأنظمة التقليدية المعتمدة على التعلم الآلي المركزي (Centralized ML) تحديات جوهرية تتعلق بانتهاك خصوصية بيانات المستخدمين.

في هذا السياق، ظهر التعلم الفيدرالي (FL) كحل واعد يسمح بتدريب النماذج بصورة تعاونية دون الحاجة الى نقل البيانات الخام مما يسهم في تعزيز خصوصية البيانات وأمن الشبكات. ومع ذلك، يواجه التطبيق المباشر للتعلم الفيدرالي تحديات حقيقية، أبرزها مشكلة عدم التجانس البيانات (Not Independent and Identically Distributed Data) بين العملاء، وقابلية التعرض للهجمات العدائية مثل هجمات التسميم (Poisoning Attacks) التي تهدف إلى إفساد النموذج الفيدرالي.

تقدّم هذه الرسالة إطار عمل فيدرالي جديد وفعال لكشف التطفل، أُطلق عليه اسم FedID (Federated Intrusion Detection)، قادر على العمل بكفاءة في بيئات واقعية تتسم بوجود توزيع بيانات غير متجانس وعملاء ضارّين. يعتمد الإطار المقترح على بنية دفاعية متقدمة تجمع بين آلية اختيار العملاء قائمة على السمعة، وخوارزمية تجميع مرجحة بالأداء، بهدف تقييم موثوقية مساهمات العملاء وتقليل تأثير التحديثات الخبيثة بفعالية أثناء عملية التعلم. كما تم اعتماد مصنّف يعتمد على الشبكات العصبية الالتفافية أحادية البعد (1D-CNN) كنموذج أساسي للتصنيف وأستخراج الخصائص الشبكية.

لتقييم أداء إطار العمل، أجريت سلسلة من التجارب المكثفة باستخدام ثلاث مجموعات بيانات معيارية (NSL-KDD, NF-BoT-IoT-V2, inSDN)، تحت ثلاثة اعدادات تجريبية مختلفة لمحاكاة ظروف واقعية مختلفة. وتمت مقارنة أداء إطار عمل FedID المقترح مع الأطر فيدرالية مرجعية قائمة على خوارزمية FedAvg القياسية وخوارزمية FedProx المخصَّصة للبيئات غير المتجانسة.

أظهرت النتائج التجريبية تفوق إطار العمل FedID على الأطر الفيدرالية المرجعية من حيث الدقة والاستقرار في الأداء وسرعة التقارب، إذ حافظ على مستوى أداء مرتفع تجاوز 98% حتى في البيئات العدائية ذات التوزيع غير المتجانس.

Abstract

The massive expansion of cyberspace, the increasing reliance on digital transactions, and the proliferation of network-connected devices have led to an unprecedented rise in the volume and complexity of cyber threats. To address these threats, Intrusion Detection Systems (IDS) have emerged as a critical line of defense for protecting data and digital infrastructures. However, traditional systems based on centralized machine learning face fundamental challenges related to violations of users' data privacy.

In this context, Federated Learning (FL) has emerged as a promising solution, allowing models to be trained collaboratively without transferring raw data, thereby enhancing data privacy and network security. Nevertheless, the direct application of federated learning faces real challenges, the most notable being statistical data heterogeneity (non-IID) among clients and vulnerability to adversarial attacks such as poisoning attacks, which aim to corrupt the federated global model.

This thesis proposes a novel and effective federated intrusion detection system, termed FedID, designed to operate efficiently in realistic environments characterized by non-IID data distributions and the presence of malicious clients. The proposed system relies on an advanced defensive architecture that combines a reputation-based client selection mechanism with a performance-weighted aggregation algorithm, aiming to assess the reliability of client contributions and effectively mitigate the impact of malicious updates during the learning process. In addition, a one-dimensional Convolutional Neural Network (1D-CNN) classifier is adopted as the core model for network feature extraction and classification.

To evaluate the performance of the proposed system, a series of extensive experiments was conducted using three benchmark datasets (NSL-KDD, NF-BoT-IoT-V2, and inSDN) under three different experimental settings to simulate diverse realistic scenarios. The performance of FedID was compared against baseline federated systems based on the standard FedAvg algorithm and the FedProx algorithm, which is tailored for non-IID environments.

The experimental results demonstrate that the proposed FedID system outperforms the reference approaches in terms of accuracy, performance stability, and convergence speed, maintaining a high performance level exceeding 98% even in adversarial environments with heterogeneous data distributions.

University of Mosul
College of Education
For Pure Science

Federated Learning-Based Approach for Network Intrusion Detection Using Trusted Clients classification

Hutheifa Anwer Mohammed Hasan

M.Sc. Thesis

Computer Science

Supervised by

Asst. Prof.

Dr. Awos Khazal Ali

2025 A.D 1447 A.H