الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

Anomaly-Based Intrusion Detection System in Wireless Sensor Networks using Machine and Deep Learning Algorithms

A Thesis Submitted by

Zinab Mohammed Abdo Ali Farea

To

The Council of Postgraduate Studies and Scientific Research, in Partial Fulfillment of the Requirements for the Degree of Master of Computing in Computer Networks

Supervisor

Assoc.prof. Belal Abdullah Rassea Al-Fuhaidi

Associate prof. of Communication Engineering.

University of Science and Technology

January, 2026AD **Sana'a** **Rajab, 1447AH**

الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

Abstract

One of the most significant issues in Wireless Sensor Networks (WSNs) is security, which must address to keep WSNs safe from malicious attacks. An Intrusion Detection System (IDS) is essential in analyzing network traffic and detecting abnormal events. However, these IDSs suffer from several drawbacks that affect their effectiveness and flexibility in accuracy, so they must overcome these to improve IDS performance. These drawbacks include difficulties in determining the appropriate dataset, the problem of feature selection, the issue of the imbalanced dataset, and choosing suitable algorithms for the classification process in WSN. This research proposed a model for an anomaly-based IDS in WSNs. This model applied mutual information (MI) for feature selection and the synthetic minority oversampling technique (SMOTE) to solve the imbalanced dataset problem. It used different machine learning (ML) (random forest (RF), decision tree (DT), support vector machine (SVM), and k nearest neighbors (KNN)) and deep learning (DL) deep neural network (DNN) algorithms to analyze network traffic and classification binary or multi-classification. To implement and measure the performance of the proposed model, relying on the standard dataset NSL-KDD. Python language is used in the Anaconda platform, and many metrics to evaluate and measure the performance of the proposed model. Experimental results show that the proposed model can accurately detect intrusion using ML and DL algorithms. The results of the proposed model for different algorithms achieved better performance than the state-of-the-art, the maximum enhancement reached 15%.

Candidate

Zinab Mohammed Abdo Ali Farea

Supervisor

Dr. Belal Abdullah Rassea Al-Fuhaidi
Associate prof.of Communication Engineering.
University of Science and Technology

January, 2026AD **Sana'a** **Rajab, 1447AH**

الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

المُلخص

يعد الأمان أحد أكثر المشكلات أهمية في شبكات الاستشعار اللاسلكية (WSNs) ، والذي يجب معالجته للحفاظ على شبكات WSN آمنة من الهجمات الضارة. يمكن أن يلعب نظام كشف التسلل(IDS) دورًا مهمًا في تحليل حركة مرور الشبكة واكتشاف الأحداث غير الطبيعية. ومع ذلك ، فإن الانظمة الحالية لكشف التسلل (IDS) تعاني من العديد من العيوب التي تؤثر على فعاليتها ومرونتها وتؤثر على دقة الاكتشاف ، لذلك يجب التغلب عليها لتحسين أداء انظمة كشف التسللIDS. تشمل هذه العيوب الصعوبات في تحديد مجموعة البيانات المناسبة ، ومشكلة اختيار الميزات، ومشكلة مجموعة البيانات غير المتوازنة ، واختيار الخوارزميات المناسبة لعملية التصنيف في WSN. في هذا البحث ، نقترح نموذجًا ذكيا لنظام IDS يعتمد على التغير في سلوك شبكة الـWSN. يطبق هذا النموذج تقنية اختيار الميزات والانماط باستخدام تقنية ترشيح المعلومات المتبادلة (MI) لاختيار الميزة، وتقنية فرط عينات الأقليات الاصطناعية (SMOTE) لحل مشكلة مجموعة البيانات غير المتوازنة. ويتم استخدم خوارزميات مختلفة للتعلم الآلي (ML) (الغابة العشوائية (RF) وشجرة القرار(DT) و الة المتجهات الداعمه (SVM) و الجار الاقرب (KNN)) والتعلم العميق (DL) (الشبكه العصبية العميقة (DNN)) لتحليل حركة مرور البيانات في الشبكة وتصنيف الهجمات الى ثنائي: "طبيعي أو هجوم" , ومتعدد: "طبيعي أو هجوم متنوع". لتنفيذ وقياس أداء النموذج المقترح ، اعتمدنا على مجموعة البيانات القياسية NSL-KDD ، واستخدمنا لغة Python في منصة Anaconda ، واستخدمنا العديد من المقاييس لتقييم أداء النموذج المقترح وقياسه. تظهر النتائج التجريبية أن النموذج المقترح يمكنه اكتشاف التسلل بدقة عالية باستخدام خوارزميات ML و DL. حيث و قد حققت نتائج النموذج المقترح للخوارزميات المختلفة أداءً أفضل مقارنةً بأحدث ما توصلت اليه انظمة وتقنيات كشف التسلل الحالية، وبلغ الحد الأقصى للتحسين 15٪.

الطالب

زينب محمد عبده علي فارع

المشرف

أ. د. بلال عبدالله راصع الفهيدي

أستاذ هندسة الاتصالات المشارك

جامعة العلوم والتكنولوجيا

يناير، 2026م **صنعاء** **رجب، 1447هـ**

الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

كشف أحداث التسلل غير الطبيعية في شبكات الاستشعار اللاسلكية باستخدام خوارزمية التعلم الآلي والعميق

رسالة مقدمة من الطالب

زينب محمد عبده علي فارع

إلى

مجلس الدراسات العليا والبحث العلمي، وهي جزء من متطلبات الحصول على درجة الماجستير في الحوسبة ـ شبكات الحاسوب

المشرف

أ. د. بلال عبدالله راصع الفهيدي
أستاذ هندسة الاتصالات المشارك
جامعة العلوم والتكنولوجيا

يناير، 2026م صنعاء رجب، 1447هـ