جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب وشبكاتها

تطوير نظام كشف التسلل في الشبكات اللاسلكية باستخدام التعلم العميق

Development of an intrusion detection system in wireless networks using deep learning

م. زين امير حربا
د. مفيد حداد

الملخص

يعتبر أمن الشبكات من المواضيع الهامة لحماية الشبكات والمنظمات والافراد وتحديدا عند تبادل معلومات مهمة، ويكون دور نظام كشف التسلل هو اتخاذ القرار المناسب لحماية المعلومات ولتحقيق ذلك تم استخدام خوارزميات التعلم العميق في هذا البحث.

يعمل هذا البحث على تطبيق خوارزميتين من خوارزميات التعلم العميق لكشف التسلل على الشبكات اللاسلكية، وهما الشبكة العصبونية التلافيفية convolutional neural networks (CNN)وشبكة الذاكرة طويلة قصيرة المدى long short term memory (LSTM)، تعمل هاتان الخوارزميتان على الحصول على أعلى معدل كشف للتسلل على الشبكات اللاسلكية ولتقليل معدل الإنذارات الكاذبة.

تم في هذا البحث اقتراح خوارزمية جديدة CNN-LSTM IDSوذلك بدمج الخوارزميتين حيث تم حقن الخوارزمية LSTM في مرحلة من مراحل تطبيق الخوارزمية CNNوذلك لاكتشاف التسلل في الشبكات اللاسلكية باستخدام التعلم العميق، حيث تم تنجيز الخوارزمية في بيئة المحاكاة anaconda باستخدام لغة python واختبرت الخوارزمية بالاعتماد على NSL_KDD_dataset التي تعتبر مجموعة بيانات شاملة تسهل عملية مقارنة النتائج.

القسم النظري

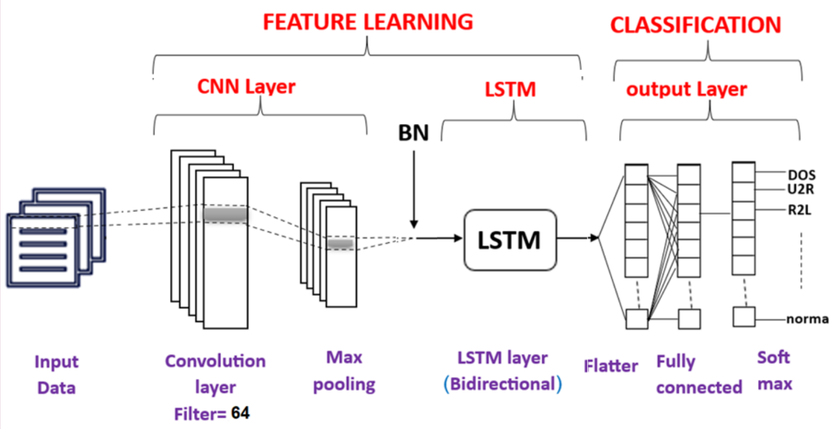
التعلم العميق: هو أحد فروع التعلم الآلي الذي يتعامل مع أنواع مختلفة من الشبكات العصبونية الاصطناعية مع أكثر من طبقة مخفية، تم استخراج بيانات التدريب والاختبار المستخدمة في هذا العمل البحثي من مجموعة بياناتNSL-KDD ،

الشبكات العصبونية التلافيفيةConvolutional Neural Network (CNN) : تعمل على استخراج الميزات الأكثر أهمية وتتكون من طبقات متعددة وتستخدم بشكل أساسي لمعالجة الصور واكتشاف الأشياء كما أثبتت كفاءتها ي اكتشاف التسلل.

شبكات الذاكرة طويلة قصيرة المدى Long Short-Term Memory (LSTMs): هي نوع محسن من الشبكات العصبونية التكرارية (RNN) التي يمكنها تعلم وحفظ المعلومات طويلة المدى، الهدف الرئيسي من تصميمها هو تفادي مشاكل الشبكات العصبونيّة التكرارية RNN البسيطة والحصول على نتائج أفضل، تحتفظ شبكة LSTMs بالمعلومات بمرور الوقت.

هجمات الشبكةNetwork Attacks : تم تصنيف الهجوم النشط إلى فئات مختلفة وهي : ١- رفض الخدمة Denial of Service (DoS) :يجعل المهاجم موارد الشبكة او الذاكرة مشغولة او ممتلئة حيث لا يمكن الاستجابة للطلبات المشروعة، او يتم رفض وصول المستخدم الى الجهاز.٢- رفض الخدمة الموزعة (DDoS) :يشبه DDoS هجمات DoS باستثناء أن الخدمة مليئة بالطلبات من خوادم متعددة لجعل المحاولة أكثر كفاءة ودقة .٣- التحقيق(Probe) : يتضمن هذا النوع من الهجمات الحصول على معلومات حول مستخدم بعيد من الشبكة، تم تصميمه عمدًا من قبل مهاجم ليطبق على ضحية مستهدفة. ٤- الجذر إلى الجهاز المحلي (R2L) :تحدث عندما يقوم المهاجم الذي يملك القدرة على ارسال الحزم الى جهاز معين في الشبكة لكنه لا يملك حساب على هذا الجهاز باستغلال نقاط الضعف لكسب الوصول المحلي كمستخدم على ذلك الجهاز. . ٥- المستخدم إلى الجذر (U2R) :هو الوصول غير القانوني إلى امتيازات المستخدم المحلي، يقوم المهاجم بالوصول إلى حساب مستخدم طبيعي على النظام وقادر على استغلال بعض نقاط الضعف لاكتساب وصول الجذر إلى النظام.

القسم العملي



المرحلة الأولى هي استيراد البيانات (بيانات التدريب والاختبار) والمعالجة المسبقة لها، وازالة القيم المفقودة والتكرارات ان وجدت، يتم تصنيف البيانات الثنائية المستهدفة التي تمثل السجلات إلى عادية أو هجومية (عادية = 0 وهجوم = 1)، وترميز البيانات الفئوية، وتمرير البيانات كمصفوفةNumPy ، تم تقسيم البيانات باستخدام خاصية kfoldوذلك للتحقق من دقة النظام بعد تصميم النموذج، تم تدريب البيانات على نموذج التعلم العميق المقترح وتقييم النتائج، وبعد ذلك تم الحصول على الدقة ومصفوفة الارتباك وتقرير التصنيف.

بنية النموذج المقترح: ١- Input layer: قبل تقديم البيانات الى النموذج المقترح ليتم تطبيقه يجب اجراء عملية المعالجة المسبقة للبيانات.

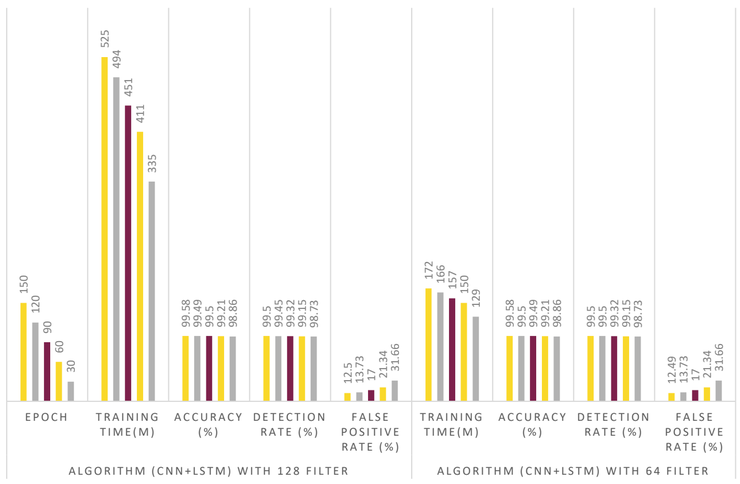
٢-Convolution layer: الهدف الأساسي لهذه الطبقة هو القيام بعملية استخراج الميزات extract features.

٣- Batch normalization: تعمل على توحيد output distribution لكل الطبقات حيث تتوضع بين كل طبقتين وتعمل على تسريع معدل التعلم وتقليل عدد ال epoch.

٤- Bidirectional LSTM layer: تعمل هذه الطبقة على تذكر المعلومات المهمة وتحسين جودة الخرج.

٥- Output layer: في طبقة الخرج تم استخدام عدد من التوابع التي تعمل على تحسين دقة التصنيف ومعدل مقاييس التقييم .

النتائج والمناقشة



تم مناقشة عدد من الحالات والتعديلات على الخوارزمية المقترحة:

- الحالة الأولى: تم استخدام طبقة CNNتحوي على 64مرشح وكذلك تم دمج طبقة LSTM تحوي 64مرشح.
- الحالة الثانية: تم استخدام طبقة CNN تحوي على 128مرشح وكذلك تم دمج طبقة LSTM تحوي 128مرشح.

الحالتين الأولى والثانية تعمل على تقليل عدد الطبقات لتقليل تعقيد النظام وتناقش عدد الفلاتر المستخدمة في كل من الحالتين بما يتناسب مع قاعدة البيانات المستخدمة.

نتيجة: مع استخدام عدد الفلاتر 128 زيادة كبيرة في زمن التدريب ومع عدد الفلاتر 64 يقل زمن التدريب وذلك مع ملاحظة عدم التأثير على بقية معايير التقييم الأخرى، كما نلاحظ تفوق الحالة الأولى وذلك لأنها تقدم زمن تدريب منخفض دون التأثير على معدلات التقييم المعيارية الأخرى.

وبمقارنة النتائج بين الخوارزميتين تبين انه يجب تقليل عدد الفلاتر بما يتناسب مع قاعدة البيانات للحصول على زمن تدريب منخفض كما انه لا يؤثر على معدلات التقييم حيث تبين ان زيادة عدد الفلاتر في كل طبقة يزيد زمن التدريب.

المراجع

- [1] J. Hu, Ch. Liu, and Y. Cui “An Improved CNN Approach for Network Intrusion Detection System” Xidian University, China, May ,31, 2021
- [2] Z. HU, L. WANG, Y LI, W. YANG “A Novel Wireless Network Intrusion Detection Method Based on Adaptive Synthetic Sampling and an Improved Convolutional Neural Network in IEEE”, Xinjiang University, November 9, 2020
- [3] S.M. Kasongo, Y. Sun, (2020), “A Deep Long Short-Term Memory based classifier for Wireless Intrusion Detection System”, ICT Express 6 (2020) 98–103
- [4] S. Shende, S. Thorat, (2020), “Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security”, Vol.9Issue 06, June-2020