كشف هجمات حجب الخدمة الموزعة على الشبكات المعرفة برمجياً باستخدام التعلم العميق

م. وسام العلي د. حسين طياوي بحبوح

ملخص

يهدف هذا البحث إلى تطوير منهجية فعّالة لكشف ومنع هجمات حجب الخدمة الموزعة (DDoS) في الشبكات المعرفة برمجياً (SDN) باستخدام تقنيات التعلم العميق. إذ تبدأ الدراسة باستعراض الطرق السابقة المتبعة في كشف هذه الهجمات، وتحليل مدى كفاءتها عند تطبيقها في بيئة SDN. وبناءً على القصور الموجود في الطرق التقليدية، يقترح البحث نموذجاً يعتمد على الشبكات العصبية العميقة، وتحديداً الوحدات التكرارية المبوبة (GRU)، حيث تم تدريب النموذج باستخدام قاعدة بيانات CICDDoS2019. وعليه، تم تقييم فعالية الطريقة المقترحة من خلال معايير الدقة، الإحكام، والاسترداد، بالإضافة إلى اختبار النموذج في بيئة محاكاة باستخدام Mininet. وعليه فقد أظهرت النتائج تفوق النموذج المقترح، حيث حقق نسبة كشف وصلت إلى 99% في السيناريوهات القياسية، مع استقرار ملحوظ مقارنة بالطرق التقليدية. وتوصل البحث إلى أن استخدام التعلم العميق يعزز بشكل كبير من أمان واستقرار الشبكات المعرفة برمجياً، موصياً بإجراء مزيد من الدراسات حول الهجمات المعقدة في بيئات الشبكات الواسعة.

الكلمات المفتاحية:

هجمات حجب الخدمة الموزعة، الشبكات المعرفة برمجياً، التعلم العميق، منع هجمات حجب الخدمة، حجب الخدمة.

Detecting DDoS Attacks on Software-Defined Networks Using Deep Learning

Eng. Wesam Alali **Dr. Hussein Teiawi Bahbouh**

Abstract

This research aims to develop an effective methodology for detecting and mitigating Distributed Denial of Service (DDoS) attacks in Software-Defined Networks (SDN) using deep learning techniques. The study begins by reviewing existing detection methods and analyzing their efficiency within SDN environments. Addressing the limitations of traditional approaches, the paper proposes a model based on Deep Neural Networks, specifically utilizing Gated Recurrent Units (GRU). The model was trained using the CICDDoS2019 dataset. The effectiveness of the proposed method was evaluated using Accuracy, Precision, and Recall metrics, alongside validation in a simulation environment using Mininet. Experimental results demonstrate the superiority of the proposed model, achieving a detection rate of up to 99% in standard scenarios, with notable stability compared to conventional methods. The research concludes that leveraging deep learning significantly enhances the security and stability of SDNs, recommending further investigation into complex attacks within wide network environments. The research concluded that the proposed

method is effective in detecting and preventing distributed denial of service (DDoS) attacks in software-defined networks (SDN). The researcher recommended conducting more studies in this field to support the results of the study.

Keywords:

DDoS attacks, Software-defined networks, Deep learning, DDoS prevention, Denial of service.

1- المقدمة:

شهدت البنية التحتية للشبكات خلال العقد الأخير توسعًا سريعًا في عدد الأجهزة المتصلة، مما زاد من التعقيد الإداري وخلق عقبات أمام الابتكارات المستقبلية.[1] وفي ظل هذه التحديات، ظهرت الشبكات المعرفة بالبرمجيات (SDN) كنموذج مبتكر يفصل بين مستوى التحكم (Control Plane) ومستوى البيانات (Data Plane)، مما يتيح إدارة مركزية ومرنة للشبكة.[2]

ومع ذلك، وبالرغم من الميزات العديدة التي توفرها SDN، فإن مركزية التحكم تجعلها هدفاً جذاباً للهجمات السيبرانية، وأخطرها هجمات حجب الخدمة الموزعة (DDoS). تهدف هذه الهجمات إلى استنزاف موارد وحدة التحكم (Controller) من خلال إغراقها بطلبات وهمية، مما يؤدي إلى شلل كامل في الشبكة. [3]

تكمن مشكلة البحث في أن أنظمة الكشف التقليدية (IDS) غالباً ما تعتمد على قواعد ثابتة[4] أو تحليل إحصائي بسيط[5]، مما يجعلها غير قادرة على مواكبة تطور الهجمات الحديثة أو التعامل مع الأحجام الهائلة للبيانات في شبكات SDN دون التأثير على الأداء.[6] ومن هنا تنبع الحاجة الملحة إلى استخدام تقنيات أكثر ذكاءً وتكيفاً مثل التعلم العميق (Deep Learning)، الذي يمتلك القدرة على استخراج الأنماط المعقدة من حركة المرور الشبكية والتمييز بين السلوك الطبيعي والهجومي بدقة عالية واستجابة سريعة، وهو ما يسعى هذا البحث لتحقيقه.

2- أهداف البحث وأهميته:

يهدف هذا البحث إلى معالجة واحدة من أبرز التحديات الأمنية التي تواجه الشبكات المعرفية برمجياً، وهي هجمات حجب الخدمة الموزعة (DDoS)، وذلك من خلال توظيف تقنية التعلم العميق .تعتبر الشبكات المعرفية برمجياً من الحلول المبتكرة التي تسمح بإدارة وتحكم أكثر كفاءة بالشبكات، ولكن هذه الميزة تجعلها أيضًا عرضة للهجمات الإلكترونية، وبخاصة الهجمات التي تسعى لإحداث شلل في الخدمة عبر استغلال موارد الشبكة بشكل مفرط .هجمات حجب الخدمة الموزعة تشكل تهديدًا حقيقيًا لاستمرارية عمل الشبكات، حيث يمكن لمهاجمين متعددين إرسال طلبات مكثفة ومفرطة في وقت واحد، مما يؤدي إلى استنفاد موارد الشبكة وتعطيلها عن العمل بشكل فعال.

يسعى هذا البحث إلى تطوير نموذج قادر على الكشف عن مثل هذه الهجمات بسرعة ودقة من خلال الاستفادة من خوارزميات التعلم العميق .يتمثل الهدف الرئيسي في استخدام شبكة عصبية عميقة تكون قادرة على التمييز بين الحركة الشبكية الطبيعية وتلك التي ترتبط بهجمات حجب الخدمة، مما يتيح القدرة على اتخاذ إجراءات وقائية واستباقية

لحماية الشبكة من التعطيل .تعتمد منهجية البحث على تدريب الشبكة العصبية العميقة باستخدام مجموعات بيانات واسعة تحتوي على سجلات للهجمات الشبكية، بالإضافة إلى حركات شبكة طبيعية، حيث يتوقع أن يسهم هذا التدريب في تطوير نموذج ذكي يتسم بقدرة عالية على التصنيف والتعرف على الهجمات في وقت مبكر.

تتجلى أهمية هذا البحث في عدة جوانب؛ أولاً، يعتبر هذا النموذج أداة متقدمة في تعزيز أمن الشبكات المعرفية برمجياً، والتي تمثل بنية تحتية أساسية للعديد من التطبيقات الحيوية، بما فيها الخدمات السحابية، وإنترنت الأشياء، وأنظمة المدن الذكية .ثانياً، يسهم البحث في توفير نظام وقائي يستند إلى خوارزميات التعلم العميق، وهو ما يعزز من كفاءة أنظمة الكشف التقليدية التي تعتمد غالباً على التحليل اليدوي أو قواعد بيانات سابقة قد تكون غير قادرة على التكيف مع طبيعة الهجمات المتطورة .ثالثاً، من خلال التدريب على مجموعات بيانات شاملة ومتنوعة، يصبح هذا النموذج مرنًا وقادرًا على التعرف على أنواع جديدة من الهجمات التي قد لا تكون معروفة سابقاً، مما يعزز من قدرته على التكيف مع التحديات المتغيرة التي تواجه الأمن السيبراني.

3- الإطار النظري:

3-1 الشبكات المعرفة برمجياً (SDN): تعتبر السمة الأكثر تميزًا في بنية SDN مقارنةً بالهياكل التقليدية هي فصل الطبقة المنطقية للتحكم عن طبقة البيانات.[2] يتحكم المستوى المركزي في عدة أجهزة شبكية موزعة، مما يوفر رؤية شاملة للشبكة. وتتألف هذه البنية من ثلاث طبقات: التطبيقات، التحكم، والبيانات، وتعتمد بشكل رئيسي على بروتوكول OpenFlow للتواصل بين وحدة التحكم والمحولات[3].

2-3 مفاهيم التعلم العميق المستخدمة: يعتمد البحث على عدة تقنيات متقدمة لتحسين أداء النموذج:

- **Dropout:**

هو تقنية تُستخدم في الشبكات العصبية لتقليل مشكلة الإفراط في التكيّف .(overfitting)يتم ذلك من خلال إيقاف عمل بعض الوحدات العُصبية بشكل عشوائي أثناء التدريب .في العرض، تم استخدام Dropoutبنسبة 0.2و 0.3في طبقات مختلفة، مما يعني أن هناك فرصة 20%و 30%لتعطيل بعض الوحدات العصبية في هذه الطبقات خلال كل خطوة تدريبية .الفكرة هي منع النموذج من الاعتماد الشديد على وحدات عصبية محددة، مما يؤدي إلى شبكة أكثر عمومية وقادرة على التكيف مع بيانات جديدة.

- **Batch Normalization:**

هي تقنية تُستخدم لتسريع عملية التدريب وزيادة استقرار الشبكة العصبية عن طريق جعل التوزيع الخاص بالمدخلات إلى كل طبقة أكثر استقراراً .تقوم Batch Normalizationبتطبيع المُدخلات بحيث يكون متوسطها صفرًا وانحرافها المعياري واحدًا قبل تمريرها إلى الطبقة التالية، مما يساعد في تحسين عملية التعلم.

- **Adam Optimizer:**

هو خوارزمية تحسين تُستخدم لتحديث الأوزان في الشبكات العصبية خلال التدريب .تعتمد على كل من معدلات التعلم التكيفية والزخم لتسريع التقارب وتقليل الخطأ .في العمل، تم استخدام

Adamبمعدل تعلم قدره 0.00004مما يعني أن التحديثات على الأوزان تتم بحذر، مما يزيد من دقة التدريب مع مرور الوقت.

- محاكي **Mininet**

محاكي Mininetهو أداة برمجية مفتوحة المصدر تُستخدم لإنشاء شبكات افتراضية تحاكي الشبكات الحقيقية .صُمم خصيصاً لتوفير بيئة اختبار مثالية لتقنيات الشبكات الحديثة، بما في ذلك الشبكات المعرفة برمجياً (SDN)والبروتوكولات الجديدة التي تحتاج إلى اختبار وتقييم قبل نشرها في بيئات حقيقية .يُستخدم Mininetبشكل واسع في الأوساط الأكاديمية والصناعية لاختبار أداء وتصميم الشبكات وتطوير البروتوكولات المختلفة.

- قاعدة البيانات وتعويض عدم التوازن باستخدام**SMOTE**

تم استخدام قاعدة بيانات CICDDoS 2019التي تحتوي على بيانات طبيعية وبيانات لهجمات DDoS.هذه البيانات غير متوازنة حيث أن الهجمات نادرة مقارنة بالبيانات العادية المولّدة كاستخدام طبيعي .لتعويض هذا التفاوت في الفئات، تم استخدام خوارزمية SMOTE (Synthetic Minority Over-sampling Technique) ، التي تُنشئ عينات اصطناعية من الفئة الأقلية)الهجمات (بناءً على المسافة الإقليدية بين نقاط البيانات .المعادلة الرياضية لـ SMOTEهي:

$$(\text{minority}x - \text{neighbor}x) \times \lambda + \text{minority}x = \text{new}x$$

- بنية الشبكة العصبية واستخدام**L2 Regularization**

الشبكة العصبية المستخدمة تعتمد على عدة طبقات تشمل طبقات من الشبكة العصبونية الالتفافية ذات البوابة –والتي تستخدم عادةً في العمليات التي تتطلب تتالي مستمر – GRU (Gated Recurrent Units) و) Denseكثيفة(، وتم تطبيق Dropoutو BatchNormalizationلتحسين الأداء .تمت إضافة L2 Regularizationلتجنب مشكلة الإفراط في التكيّف .يتمثل L2 Regularizationفي إضافة مجموع مربعات الأوزان إلى دالة الخسارة، والمعادلة الرياضية هي:

$$L_{total} = L_{original} + \lambda \times \sum w^2$$

4- مواد البحث:

البرمجيات :

–لغة البرمجة بايثون Python الإصدار 3.9. (مستخدمة على نطاق واسع في تطبيقات الذكاء الاصطناعي) [python Docs]

–المكتبة البرمجية تينسورفلو TensorFlowالإصدار 2.7.[6]

–المكتبة البرمجية كيراس Kerasالإصدار 2.7.0. [6]

–المكتبة البرمجية بانداس Pandasالإصدار 1.3.5. [4]

العتاديات:

بيئة المخبر الموفرة من غوغل Colab

المعالج: 2vCPU @ 2.2GHz

ذاكرة النفاذ العشوائي RAM المثبتة: 13GB RAM

معالجة بيانات قاعدة البيانات:

-تقسيم مجموعة البيانات إلى أجزاء أصغر.

-معالجة حالات الادخال الخاطئة وحذفها.

-معالجة قيم الادخال الأوسع من مجال تخزين القيم العددية.

-معالجة كل القيم لتصبح في المجال من 0وحتى) 1يشمل ذلك منفذ الهجوم وعنوان الجهاز المهاجم وهو ما كان يتم تجاهلهما في الدراسات السابقة المعتمدة على خوارزميات التعلم العميق.

-اعتماد قيمة 1لاعتبار الجهاز كمهاجم و 0لاعتباره مستخدم طبيعي.

مقاييس الأداء:

الدقة Accuracy: هي مقياس يمثل نسبة التوقعات الصحيحة إلى إجمالي التوقعات .

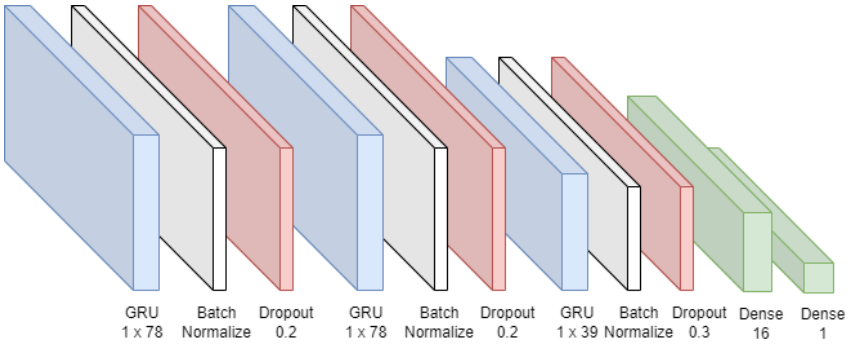
الإحكام (Precision): نسبة التوقعات الإيجابية الصحيحة إلى جميع التوقعات الإيجابية .يُستخدم لقياس مدى دقة النموذج في تحديد الفئات الإيجابية

الاسترجاع أو الحساسية (Recall): يُشير إلى نسبة التوقعات الإيجابية الصحيحة إلى جميع الفئات الإيجابية الحقيقية .يُستخدم لقياس قدرة النموذج على استرجاع الفئات الإيجابية.

مستوى F1 (F1 Score): هي مقياس يجمع بين الاحكام والاسترجاع في قيمة واحدة. تُستخدم لتوفير توازن بينهما، خاصة عندما تكون البيانات غير متوازنة.

5- النتائج والمناقشة:

المخطط البنيوي للشبكة:



الشكل (1) المخطط الصندوقي في الصورة يمثل بنية نموذج شبكة عصبية يعتمد على وحدة الـ (Gated Recurrent Unit) GRU، ويحتوي على طبقات متعددة تساعد في التعامل مع البيانات التسلسلية)مثل النصوص، وسلاسل البيانات الزمنية (لتحليلها أو التنبؤ بالأنماط.

6- التفاصيل حول بنية النموذج:

1. **مبررات اختيار نموذج GRU** : تم اختيار الوحدات التكرارية المبوبة (GRU) بدلاً من الذاكرة طويلة المدى (LSTM) أو الشبكات الالتفافية (CNN) لعدة أسباب جوهرية. على الرغم من أن LSTM فعالة في التعامل مع التسلسلات الزمنية، إلا أن GRUتمتاز ببنية أبسط (بوابات أقل)، مما يجعلها أسرع في التدريب وأقل استهلاكاً للموارد الحسابية، وهو عامل حاسم في بيئات SDN التي تتطلب كشفاً في الوقت الحقيقي (Real-time detection)وتأخيراً (Latency) منخفضاً.
2. **طبقات GRU**:
   - هناك طبقتان من وحدات GRU، كل منهما تحتوي على 78و 39وحدة (nodes)على التوالي .وحدات GRUتُستخدم كطبقات متكررة في الشبكات العصبية لتحليل البيانات الزمنية

أو المتتابعة .تم تصميم هذه الوحدات خصيصاً للحفاظ على المعلومات في الوقت الذي تتقدم فيه عبر التسلسل، مما يجعلها مفيدة للمهام التي تتطلب تذكر السياق.

- الطبقة الأولى تحتوي على شكل (78 × 1)من الوحدات، والطبقة الثانية (39 × 1)، ما يشير إلى عدد الوحدات في كل طبقة.

3. التطبيع بالدفعات (Batch Normalization):

- بين طبقات GRU، توجد طبقات لتطبيع الدفعات .تطبيع الدفعات يُستخدم لتسريع عملية التدريب وجعل النموذج أكثر استقراراً، حيث يقوم بتطبيع مدخلات الطبقة القادمة على أساس القيم المتوسطة والانحراف المعياري لكل دفعة بيانات .هذا يساعد في تجنب مشاكل التشبع وتسريع عملية الانتشار الخلفي.

4. الانسحاب(Dropout) :

- هناك طبقات انسحاب (Dropout) تم تطبيقها بعد كل طبقة تطبيع .النسبة المستخدمة هي 0.2و0.3، مما يعني أن النموذج سيقوم بتعطيل 20% و 30%من الوحدات في كل دفعة أثناء التدريب بشكل عشوائي لتجنب فرط التكيف (overfitting)، بحيث يعتمد النموذج على مجموعة متنوعة من الوحدات ولا يتوقف على وحدات محددة.

5. الطبقات الكثيفة(Dense Layers) :

- بعد طبقات GRU والتطبيع والانسحاب، تأتي طبقتان كثيفتان .الطبقة الأولى تحتوي على 16 وحدة، والأخيرة تحتوي على وحدة واحدة فقط .تُستخدم الطبقات الكثيفة لتجميع المعلومات من الطبقات السابقة وتوليد التنبؤ النهائي .في هذه الحالة، يبدو أن الطبقة النهائية تُستخدم للحصول على مخرج نهائي، وهو ناتج رقمي قد يكون له علاقة بالتنبؤات أو التصنيفات المطلوبة.

7- تفسير العمل العام للنموذج:

هذا النموذج مصمم للتعامل مع البيانات المتتابعة، حيث تقوم طبقات GRUبمعالجة التسلسل واستخراج الميزات الزمنية .يتم تطبيع البيانات عند كل طبقة، وتطبيق الانسحاب لتجنب فرط التكيف .في النهاية، يتم تمرير النتائج إلى الطبقات الكثيفة لتجميع الميزات المستخرجة والحصول على المخرج النهائي للنموذج.

متوسطات المحاكاة:

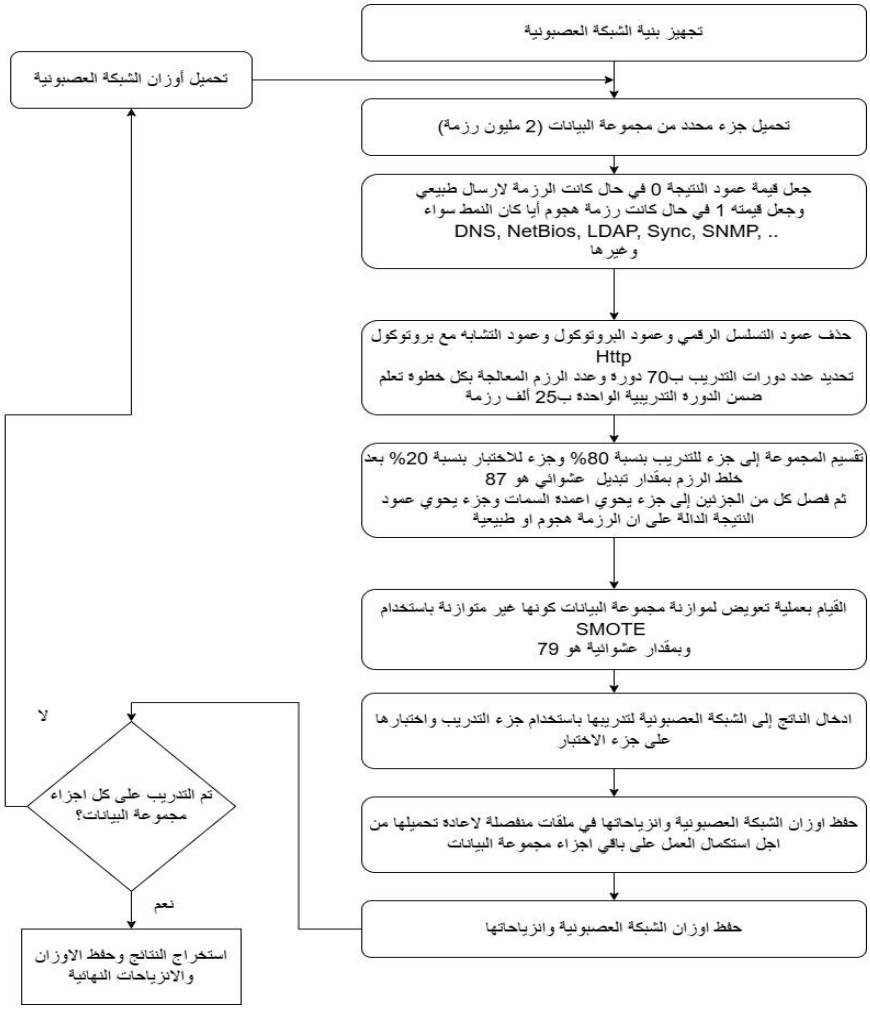
تم تحديد قيم المتوسطات بناءً على سلسلة من التجارب للوصول إلى الأداء الأمثل:

معدل التعلم (0.00004): تم اختياره بعد تجربة قيم أكبر (مثل 0.001) أدت إلى تذبذب النتائج، وقيم أصغر أدت إلى بطء شديد في التقارب. هذه القيمة وفرت التوازن الأفضل بين السرعة والدقة.

نسب Dropout (0.2 و 0.3): تم اعتماد هذه النسب المتفاوتة في الطبقات المختلفة لمنع "الإفراط في التكيف" دون فقدان الكثير من المعلومات الهامة، حيث أثبتت التجارب أن زيادة النسبة عن 0.5 تؤدي إلى انخفاض دقة النموذج (Underfitting).

الموسط	القيمة والواحدة	ملاحظات
المجموعة الجزئية	2 مليون رزمة	تتجاوز قيم المجموعة كاملة 6 مليون رزمة
عدد الدورات التدريبية	70 دورة	
معدل التعلم	0.00004	
قيمة المنظم (regularizer) في كل طبقة	0.022	
قيمة عشوائية خوارزمية SMOTE	79	

الجدول (1)


تجهيز بنية الشبكة العصبونية
تحميل أوزان الشبكة العصبونية
تحميل جزء محدد من مجموعة البيانات (2 مليون رزمة)
جعل قيمة عمود النتيجة 0 في حال كانت الرزمة لارسال طبيعي
وجعل قيمته 1 في حال كانت رزمة هجوم أيا كان النمط سواء
DNS, NetBios, LDAP, Sync, SNMP, ..
وغيرها
حذف عمود التسلسل الرقمي وعمود البروتوكول وعمود التشابه مع بروتوكول
Http
تحديد عدد دورات التدريب ب70 دوره وعدد الرزم المعالجة بكل خطوه تعلم
ضمن الدوره التدريبية الواحده ب25 ألف رزمة
تقسيم المجموعة إلى جزء للتدريب بنسبة 80% وجزء للاختبار بنسبة 20% بعد
خلط الرزم بمقدار تبديل عشوائي هو 87
ثم فصل كل من الجزئين إلى جزء يحوي اعمده السمات وجزء يحوي عمود
النتيجة الدالة على ان الرزمة هجوم او طبيعية
القيام بعملية تعويض لموازنة مجموعة البيانات كونها غير متوازنة باستخدام
SMOTE
وبمقدار عشوائية هو 79
ادخال الناتج إلى الشبكة العصبونية لتدريبها باستخدام جزء التدريب واختبارها
على جزء الاختبار
حفظ اوزان الشبكة العصبونية وانزياحاتها في ملفات منفصلة لاعاده تحميلها من
اجل استكمال العمل على باقي اجزاء مجموعة البيانات
حفظ اوزان الشبكة العصبونية وانزياحاتها
لا
تم التدريب على كل اجزاء
مجموعة البيانات؟
نعم
استخراج النتائج وحفظ الاوزان
والانزياحات النهائية

الشكل (2)

المخطط التدفقي:

المخطط التدفقي يمثل عملية إعداد بيانات التدريب وتطبيقها على نموذج شبكي عصبي للتعرف على هجمات حجب الخدمة الموزعة (DDoS) ضمن الشبكات المعرفية برمجياً (SDN) باستخدام التعلم العميق .سأقوم بتوضيح خطوات المعالجة المشار إليها في المخطط كالتالي:

1) **تجهيز بنية الشبكة العصبية:**

أول خطوة هي إعداد البنية الأساسية للنموذج الشبكي العصبي الذي سيُستخدم لتحليل البيانات والكشف عن الهجمات.

2) **تحميل جزء محدد من مجموعة البيانات:**

يتم هنا تحميل عينة من البيانات لتدريب الشبكة .توضح الصورة أن حجم العينة هو 2مليون حزمة بيانات)رزمة(؛ هذا الحجم الكبير من البيانات يتيح تدريب النموذج بشكل أفضل ليتمكن من التعرف على الأنماط المختلفة.

3) **تحديد قيم العمود المستهدف للتصنيف:**

في هذه الخطوة، يتم تخصيص عمود للتصنيف، بحيث تُعطى قيمة "0"للرزم التي تمثل حركة مرور طبيعية، وتُعطى قيمة "1"للرزم التي تمثل هجمات، مثل البروتوكولاتDNS ، NetBios، LDAP، Sync، و SNMP هذه العملية مهمة لتصنيف البيانات وتحديد ماهية كل رزمة عادية أو هجوم.

4) إزالة الأعمدة غير الضرورية:

هنا يتم حذف الأعمدة التي لا تفيد في عملية التعلم، مثل عمود التسلسل الرقمي والبروتوكول وعمود التشابه مع بروتوكول HTTP هذه الخطوة تهدف إلى تنظيف البيانات من المتغيرات التي قد تؤدي إلى إبطاء النموذج أو زيادة التعقيد دون فائدة كبيرة.

5) تحديد دورات التدريب وعدد الرزم:

يتم تحديد عدد دورات التدريب ليكون 70دورة وعدد الرزم في كل خطوة تعلم داخل الدورة التدريبية يكون 5آلاف رزمة .هذه الإعدادات تساعد في تنظيم عملية التدريب وتحقيق توازن بين الدقة وسرعة التعلم.

6) تقسيم مجموعة البيانات إلى تدريب واختبار:

تُقسم البيانات بنسبة 80% للتدريب و 20%للاختبار .يتم تقسيم البيانات لضمان أن النموذج يتم اختباره على بيانات لم يسبق له رؤيتها أثناء التدريب، مما يساعد على تقييم أدائه.

يتم اختيار 87جزءاً عشوائياً من مجموعة الرزم للهجوم والمرور الطبيعي، ثم يُعاد دمج هذه الأجزاء مع بعضها لتكوين مجموعة البيانات النهائية المستخدمة في التدريب.

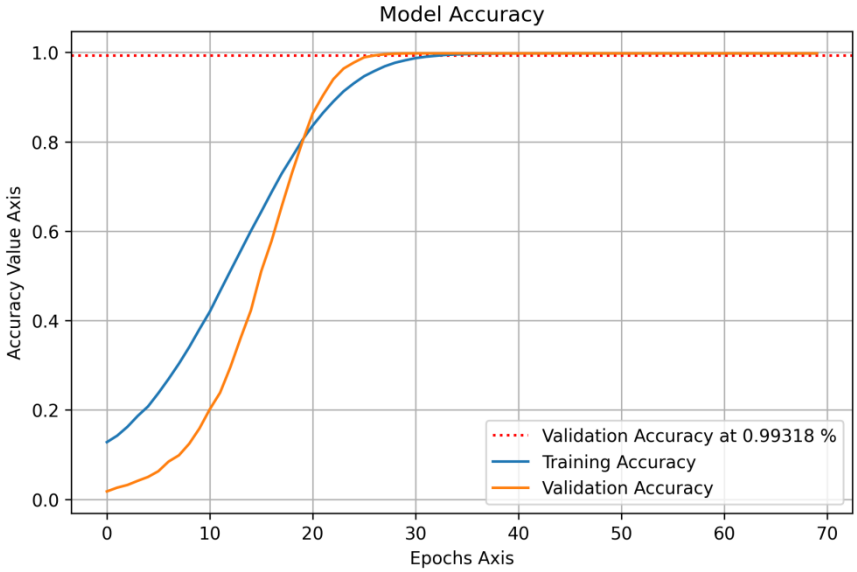
هذه العملية تساعد في تحسين دقة النموذج الشبكي العصبي في الكشف عن هجمات حجب الخدمة (DDoS) في الشبكات المعرفة برمجياً، حيث تتضمن مراحل متعددة لتنظيف البيانات، واختيار الأعمدة المهمة، وتحديد إعدادات التدريب المناسبة.

7) التعويض وتجهيز البيانات :

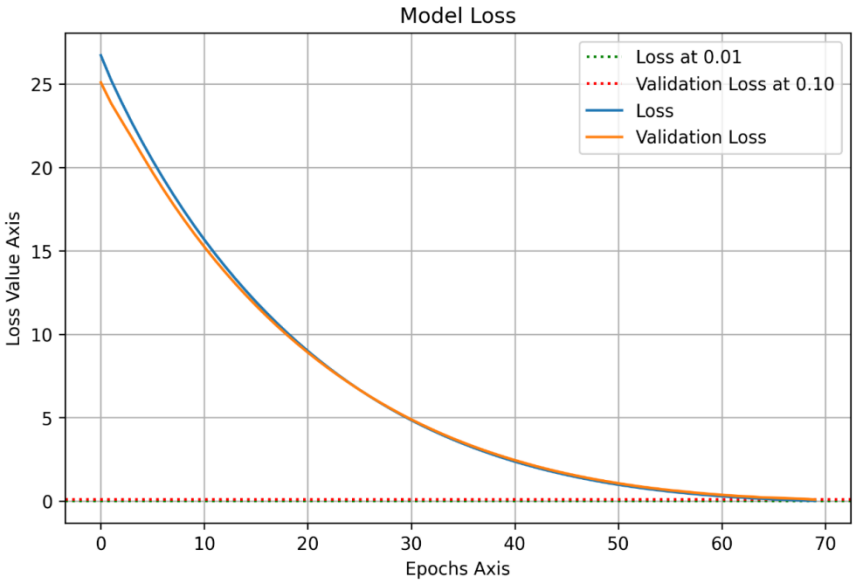
تم خلط مجموعة نهائية من الهجمات المتنوعة في مجموعة البيانات للاختبار عليها.

تم تعويض عدم توازن مجموعة البيانات باستخدام خوارزمية SMOTE.

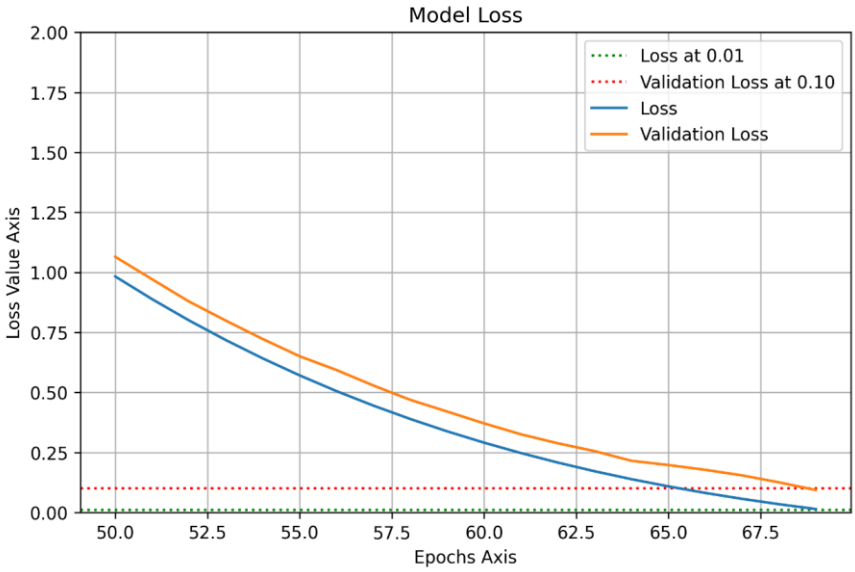
8- نتائج التدريب والاختبار :



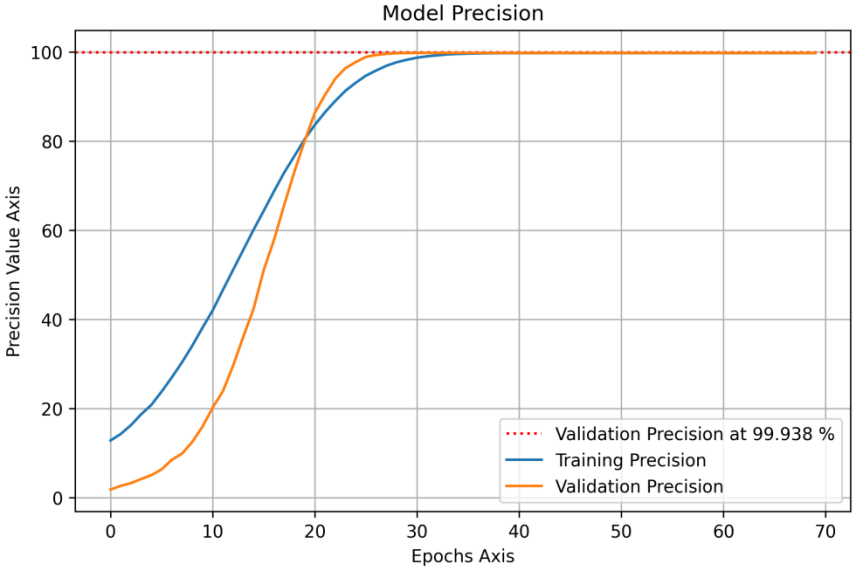
الشكل (3)


Model Loss
Loss at 0.01
Validation Loss at 0.10
Loss
Validation Loss
Loss Value Axis
Epochs Axis
0
5
10
15
20
25
0
10
20
30
40
50
60
70

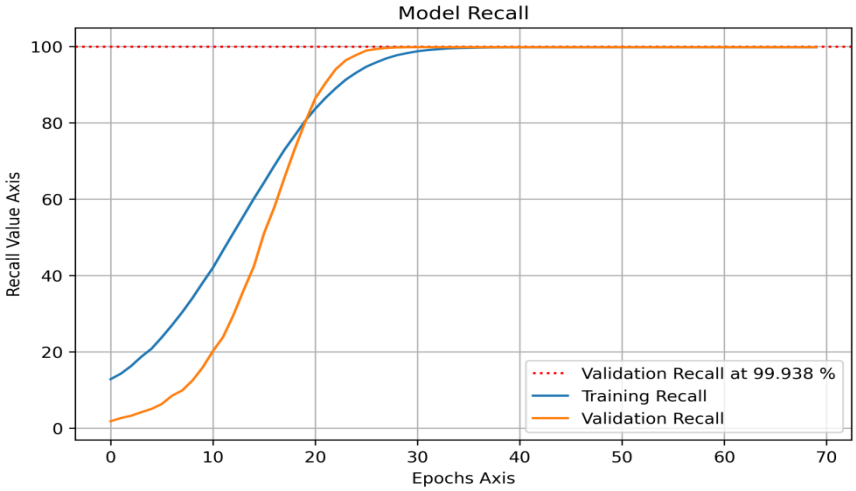
الشكل (4)



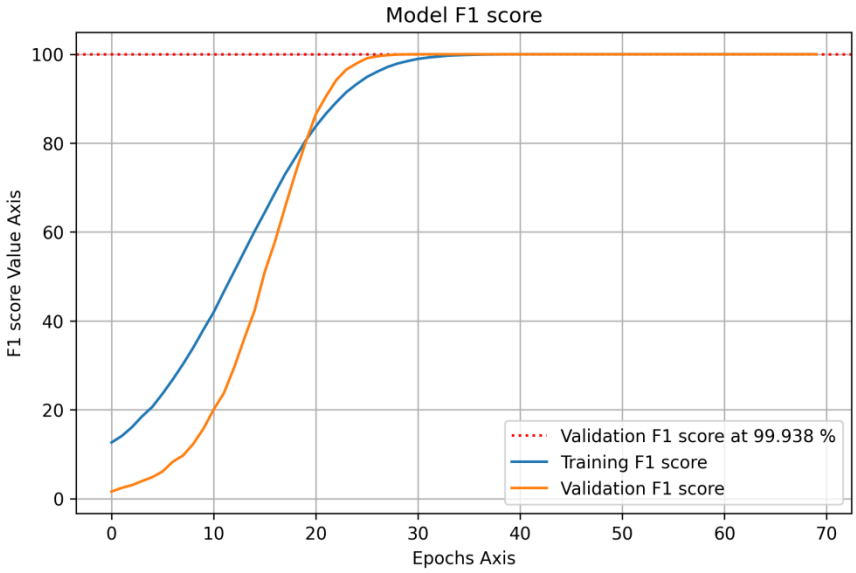
الشكل (5)



الشكل (6)



الشكل (7)

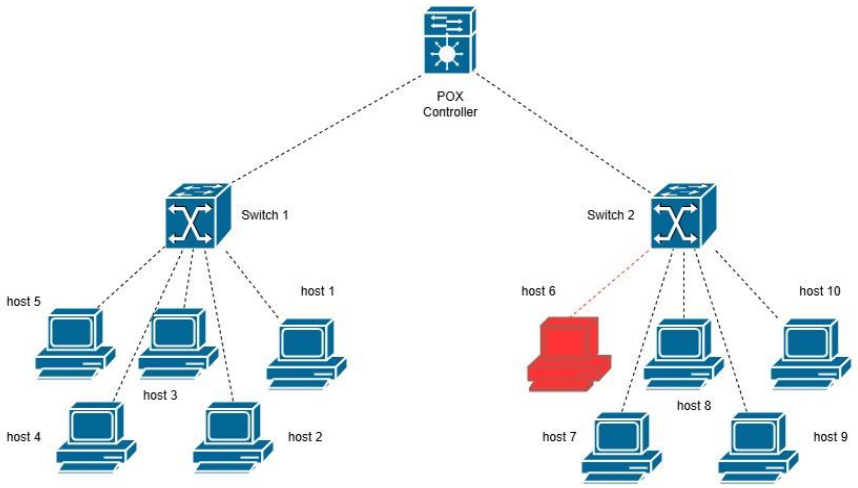


الشكل (8)

إن نتائج تدريب واختبار النموذج المقترح السابقة الذكر تظهر زيادة في عدد دورات التدريب ونلاحظ ارتفاع معدل الكشف في الاختبار عنه في التدريب لبعض المراحل.

تم بعدها بناء شبكة معرفة برمجياً محاكاة في بيئة برنامج mininet لاختبار أداء النموذج فيها في حالة الهجوم وقمنا بزيادة عدد الاجهزة في الشبكة لملاحظة التغييرات التي تحصل عند ارتفاع العدد في حالة الهجوم .تم الاختبار على شبكة تحوي 10اجهزة ومن ثم على شبكة تحتوي 100جهاز ومن ثم على شبكة تحتوي 1000جهاز .

يبين الشكل التالي بنية الشبكة في حالة ال 10اجهزة:



الشكل (9)

يمكن تلخيص النتائج التي تم الوصول إليها من عملية الاختبار في بيئة المحاكاة في الجدول التالي:

	حالة 10 اجهزة	حالة 100 جهاز	حالة 1000 جهاز	ملاحظات
نسبة الكشف	99%	99%	95%	أداء مستقر
استهلاك المعالج	40% بدون النموذج – 60% مع النموذج	75%	92%	بداية ارتفاع استهلاك الموارد
استهلاك ذاكرة الوصول العشوائي	70%	80%	95%	انخفاض في الكشف بسبب اختناق الموارد

الجدول (2)

نلاحظ انخفاض نسبة الكشف إلى 95% عند زيادة عدد الأجهزة إلى 1000. يعزى هذا الانخفاض بشكل رئيسي إلى:

- **اختناق الموارد (Resource Bottleneck)**: وصول استهلاك المعالج إلى 92% والذاكرة إلى 95% يعني أن وحدة التحكم (Controller) أصبحت مشبعة، مما يؤدي إلى تأخير في معالجة الرزم (Packet Processing Latency) أو حتى إسقاط بعضها قبل وصولها لنموذج الكشف.

- **تأثير الضوضاء (Noise):** زيادة عدد الأجهزة تزيد من تعقيد الحركة الشبكية وتداخلها، مما يرفع نسبة "الضوضاء" في البيانات المدخلة للنموذج.

- على الرغم من التركيز على دقة الكشف، إلا أن القفزة في استهلاك الموارد (من 60% إلى 92%) تشير ضمنياً إلى زيادة في زمن الاستجابة (Latency) للمعالجة. في حالة 1000 جهاز، قد يؤثر التأخير الزمني سلباً على قدرة النظام على منع الهجوم في اللحظات الأولى، وهو ما يفسر جزئياً انخفاض نسبة الكشف.

- يجب الإشارة إلى أن هذا البحث ركز على دقة الكشف (Accuracy) ومقاييس التصنيف (Precision, Recall) ولم يقم بقياس زمن الاستجابة (Latency)، وهو عامل حاسم في أنظمة الكشف الفوري. ويُعد هذا قصوراً سيتم معالجته في التوصيات.

- بمقارنة النموذج الحالي مع دراسات سابقة (مثل Ali et al. [1] التي استخدمت طرق تقليدية وحققت دقة 88%، و Elsayed et al. [10] باستخدام CNN بدقة 96%)، يتفوق النموذج الحالي في البيئات الصغيرة والمتوسطة (99%) بفضل استخدام GRU الخفيفة، بينما يبرز التحدي المشترك مع الدراسات الأخرى في الحفاظ على الأداء عند التوسع الكبير (Scalability).

9- الاستنتاجات والتوصيات:

النتائج:

- تعطي النتائج استدلالاً على تحسن مستوى الكشف ولكن بعدد مرات تدريب مرتفع نسبياً (70) دورة تدريبية

- يعزى ذلك الى ارتفاع مستوى العشوائية والتبديل المستعمل وعملية تعويض حالة عدم التوازن في مجموعة البيانات.
- ان اعتماد قيمة مرتفعة نسبياً للمنظم (regularizer) تجعل الشبكة أفضل باتجاه عدم حدوث حالة الافراط في التجهيز (overfitting) وهو ما ساهم في زيادة في عدد الدورات التي تحتاجها لتصل الى مستوى دقة مرتفع.
- نلاحظ في بعض دورات التدريب والاختبار تكون نسبة الكشف في الاختبار اعلى من التدريب وهذا بسبب القيمة المرتفعة للمنظم وكذلك آلية الحساب وهي نسبة الكشف سواء من جزء التدريب او الاختبار كما أن بيانات الهجوم في حالة الاختبار لم تتعرض لأي عملية تعويض على عكس بيانات التدريب وهو ما يضيف ضجيجاً لبيانات التدريب.
- عند الاختبار في بيئة المحاكاة نلاحظ ارتفاع استهلاك كل من قدرة المعالجة للمعالج وسعة ذاكرة الوصول العشوائي في المتحكم حتى تصل في حالة 1000جهاز إلى 92%و 95% على التوال وهي قيم مرتفعة.
- نلاحظ انخفاض نسبي بمعدل الكشف في حالة 1000جهاز وهو ما ينذر أن الزيادة اكثر ستكون ذات أثر سلبي على معدل الكشف.

التوصيات:

بناءً على الاستنتاجات السابقة، يوصي البحث بما يلي:

1- يوصى بتطوير نماذج تجمع بين تقنيات متعددة من التعلم العميق مثل الشبكات العصبية الالتفافية والتكرارية لتحسين الكشف عن الأنماط الأكثر تعقيداً في البيانات.

2- يوصى بإجراء مزيد من الأبحاث لتطوير استراتيجيات جديدة لكشف هجمات DDoS التي تستخدم تقنيات متقدمة مثل هجمات الذكاء الاصطناعي المضادة (Adversarial AI Attacks)، لضمان استدامة فعالية النظام في مواجهة التهديدات المستقبلية.

3- يوصى بقياس وتحسين زمن استجابة النموذج، كونه عاملاً حاسماً لا يقل أهمية عن دقة الكشف، خاصة في بيئات SDN التي تتطلب استجابة سريعة.

10- المراجع:

[1] Ali et al. (2020). Detecting DDoS Attack on SDN Due to Vulnerabilities in OpenFlow, Computer Science, arXiv: 1912.12221v4.

[2] Al-Amiedy, T.A.; Anbar, M.; Belaton, B.; Bahashwan, A.A.; Hasbullah, I.H.; Aladaileh, M.A.; Mukhaini, G.A. A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things. Internet Things 2023, 22, 100741.

[3] Scott-Hayward, S.; Natarajan, S.; Sezer, S. A Survey of Security in Software Defined Networks. IEEE Commun. Surv. Tutor. 2016, 18, 623-654.

[4] Ali et al. (2023). Machine Learning Techniques to Detect a DDoS Attack in SDN:A Systematic Review, Appl. Sci. 2023, 13, 3183. https://doi.org/10.3390/app13053183

[5] Mittal et al. (2023). DDoS-AT-2022: a distributed denial of service attack dataset for evaluating DDoS defense system, Proc.Indian Natl. Sci. Acad. 89, 306-324 (2023). https://doi.org/10.1007/s43538-023-00159-9

[6] Kanakam et al. (2022). DDOSDET: AN APPROACH TO DETECT DDOS ATTACKS USING NEURAL NETWORKS, arXiv:2201.09514v1.

[7] Narayan et al. (2024). A Collaborative Approach to Detecting DDoS Attacks in SDN Using Entropy and Deep Learning, Journal of Telecommunications and Information Technology.

[8] Alfatemi et al. (2024). Advancing DDoS Attack Detection: A Synergistic Approach Using Deep Residual Neural Networks and Synthetic Oversampling, arXiv:2401.03116v1.

[9] Bahashwan, A., Anbar, M., Manickam, S., Alamiedy, T., Aladaileh, M., & Hasbullah, I. (2023). A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking. Sensors (Basel, Switzerland), 23. https://doi.org/10.3390/s23094441.

[10] Elsayed et al. (2020). DDoSNet: A Deep-Learning Model for Detecting Network Attacks, arXiv:2006.13981v1.

[11] Roshan et al. (2024). Black-box Adversarial Transferability: An Empirical Study in Cybersecurity Perspective, Computer & Security Volume 141.

[12] Safaa Alali, Abdulkarim Assalem (2023). Simulation and edge computing structure in 5G, Albaath Journal volume 45, No 18.

[13] Reem Ibrahim (2024). Comparison of the accuracy of detecting security breaches on the NSL-KDD and UNSWNB15 datasets using artificial intelligence algorithms, Albaath Journal volume 46, No 10.