Journal of Engineering Sciences and Information Technology
Volume (6), Issue (6) : 30 Sep 2022
P: 15 - 36

ISSN: 2522-3321

مجلة العلوم الهندسية وتكنولوجيا المعلومات
المجلد (6)، العدد (6) : 30 سبتمبر 2022م
ص: 15 - 36

Evaluating the performance of machine learning techniques in detecting LDoS attacks in SDNs

Danial Yousef Yousef

Faculty of Mechanical & Electrical Engineering || Tishreen University || Syria

Boushra Ali Maala

Faculty of engineering || Manara University || Syria

Abstract: SDNs are still not mature enough, especially in terms of security, and can easily become a prime target for many attacks such as DoS attacks that reduce or block network services and make them unavailable to users, or they may also be a gateway to other attacks.

In this article, we present an evaluation of a set of machine learning algorithms in detecting LDoS attacks in SDNs, where cybersecurity systems can analyze and learn patterns to help prevent similar attacks and respond to changing behavior. This can help cybersecurity research teams be more proactive in preventing threats and responding to active attacks in real time.

Keywords: SDN, LDoS, ML, Cyber Security.

تقييم أداء تقنيات تعلم الآلة في كشف هجمات LDoS في شبكات SDN

دانيال يوسف يوسف

كلية الهندسة الميكانيكية والكهربائية || جامعة تشرين || سورية

بشرى علي معلا

كلية الهندسة || جامعة المنارة || سورية

المستخلص: ما تزال الشبكات المعرفة برمجيا SDN غير ناضجة كفاية وخاصة من الناحية الأمنية، ويمكن أن تصبح بسهولة هدفاً رئيساً للعديد من الهجمات كهجمات حجب الخدمة التي تسبب تقليل أو حجب خدمات الشبكة وجعلها غير متاحة للمستخدمين، أو قد تكون أيضاً بوابة لهجمات أخرى.

نقدم في هذه المقالة تقييم لمجموعة من خوارزميات التعلم الآلي في كشف هجمات LDoS في شبكات SDN، حيث يمكن لأنظمة الأمن السيبراني تحليل الأنماط والتعلم منها للمساعدة في منع الهجمات المماثلة والاستجابة للسلوك المتغير. وهذا يمكن أن يساعد فرق البحث في الأمن السيبراني على أن تكون أكثر استباقية في منع التهديدات والاستجابة للهجمات النشطة في الزمن الحقيقي.

الكلمات المفتاحية: الشبكات المعرفة برمجيا، هجوم حجب الخدمة منخفض معدل النقل، تعلم الآلة، الأمن الإلكتروني.

1- المقدمة.

أصبح الأمن السيبراني أحد مشكلات البحث الرئيسية مع تزايد خدمات الإنترنت ويتضمن تقنيات لحماية الأنظمة والأجهزة والبرامج والشبكات والبيانات الإلكترونية من الوصول غير المصرح به.

يمكن للتعلم الآلي أن يجعل تحقيق الأمن السيبراني أكثر تفاعلية، وفاعلية، وأقل تكلفة. ويمكن استخدامه في أنظمة كشف التسلل IDS Intrusion Detection System، حيث يراقب نظام كشف التسلل IDS حركة مرور الشبكة بحثاً عن أي نشاط ضار، وينبه النظام الذي ثبت عليه في حالة حدوث نشاط ضار أو تطفل، وفي أنظمة منع التطفل IPS Intrusion Prevention System حيث يتم كشف ومنع الهجمات عن طريق إسقاط رزمها وإعادة تعيين الاتصال وحظر حركة المرور وما إلى ذلك، ولكن لا يمكن تحقيق ذلك إلا إذا كانت البيانات الأساسية التي تدعم التعلم الآلي توفر وتقدم الصورة الكاملة للبيئة.

اكتشف الباحثون في SIGCOMM في عام 2003 [17, 5, 8]، نوع جديد من هجمات حجب الخدمة وهي الهجمات منخفضة معدل النقل LDoS Low-Rate Denial of Service والتي ينعكس تأثيرها في انخفاض جودة الخدمة، إن شكل هجوم LDoS هو سلسلة من النبضات الدورية الذي لا يستنزف موارد الشبكة بشكل عنيف كما في هجمات حجب الخدمة ذو المعدل العالي DoS Denial of Service، بل يستهدف الآليات التكيفية المعتمدة في بروتوكول التحكم بالتدفق TCP Transmission Control Protocol والتي تضمن الكفاءة والإنصاف لتدفقات الشبكة، مما يتسبب في تدهور استخدام الموارد لبروتوكول أو تطبيق معين، أي يتم استهداف الآليات التي من المفترض أن تحقق جودة الخدمة وتحافظ عليها بما يتناسب مع التغييرات التي تطرأ على الشبكة.

لذلك اقترحنا عدة سيناريوهات، درسنا من خلالها مجموعة خوارزميات تعلم آلي لكشف هجمات LDoS وتقييم الأداء فيما بينها.

2- مشكلة البحث:

إن عدد الدراسات التي تستهدف كشف هجمات DoS كبيرة جدا مقارنة بالدراسات التي تستهدف كشف هجمات LDoS، على الرغم من الضرر الكبير والمؤثر الذي يلحقه وخاصة عندما يستهدف وصلة مشتركة تحمل أوامر وبيانات التحكم بالإضافة إلى بيانات الشبكة في نفس الوقت.

كما أن معظم الدراسات السابقة استهدفت كشف هجمات LDoS في بيئة الشبكات التقليدية مع وجود عدد قليل جدا من الدراسات التي تهدف إلى كشف هجمات LDoS في شبكات SDN وباستخدام خوارزميات وآليات الذكاء الاصطناعي بشكل خاص.

لذلك سيتم البحث في تقييم إمكانية استخدام تقنيات تعليم الآلة في كشف هجمات LDoS في شبكات SDN.

3- فرضيات البحث:

يلعب بروتوكول التحكم في الإرسال (TCP) دوراً مهماً في الإنترنت لأنه البروتوكول المستخدم لنقل البيانات بواسطة معظم خدمات وتطبيقات الإنترنت [4].

تمثّل قناة الاتصال بين الجهازين H1 وH5 قناة الاتصال لتبادل البيانات عبر بروتوكول TCP ويتم إشغال كامل عرض الحزمة التي تقدمها هذه القناة وبنفس الوقت تستخدم الأداة IPERF لحساب قيم الإنتاجية في كل واحدة تقرير (1 ثانية)، وبالتالي تحسب العناصر للشبكة في حالة عمل الشبكة الطبيعي وحالة عمل الشبكة عند وجود الهجوم الذي يستخدم بروتوكول UDP User Datagram Protocol ثم تدريب نموذج الآلة ليتمكن من التفريق بين الحالتين.

ولكن ماذا لو استخدمت الأجهزة الشرعية بروتوكول UDP بحسب السيناريو السابق ستعتبر الآلة حركة مروره على أنها هجوم وبذلك سيتم التصنيف بشكل خاطئ، وعليه درسنا سيناريو آخر عند وجود قناة اتصال بين أحد المستخدمين H2 أو H3 يتصل مع المستخدم H4 عبر قناة اتصال ويتم تبادل البيانات عبر بروتوكول UDP ثم تحسب العناصر features وتضاف إلى قاعدة البيانات لتعليم الآلة على التفريق بين حالة عمل الشبكة الطبيعية بوجود مستخدمين يعملان ببروتوكول TCP وUDP على التوازي ثم حالة وجود الهجوم في ظل عمل البروتوكولين.

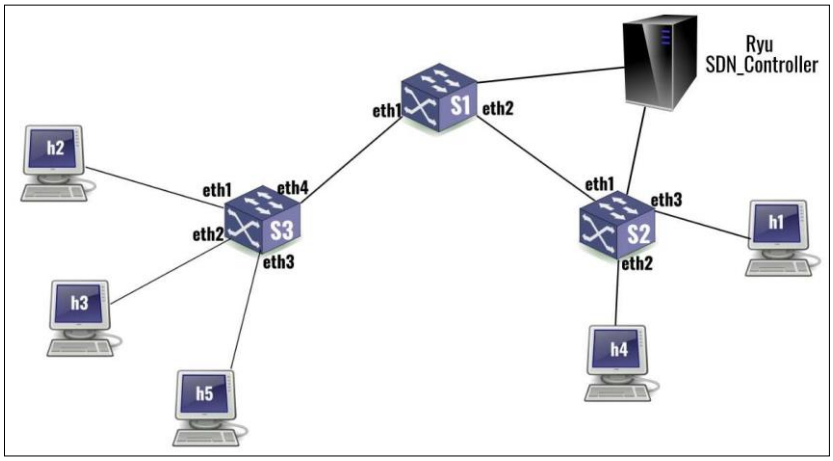
سينفذ السيناريوهان الآتيان على شبكة SDN التي تظهر في الشكل (1) التالي والمؤلفة من:

5 أجهزة Hosts، 3 مبدلات ومتحكم SDN controller)المتحكم Ryu)، وبالنسبة للتوصيلات:

أعدّت الوصلات بين العناصر باستثناء الوصلة بين المبدل S1 والمبدل S3 بعرض حزمة يساوي Gbps 1 وهي أكبر قيمة يدعمها الـ Mininet مع وجود تأخير بقيمة ms 15والحد الأقصى لاستيعاب رتل الانتظار هو frames 100000.

الوصلة S3 -S1 بعرض حزمة Mbps 500 وتأخير ms 30 وحد أقصى لاستيعاب رتل الانتظار هو frames10000، وهي بالتالي تمثل وصلة عنق زجاجة لأنها تقدم عرض حزمة أقل من عرض حزمة كل الوصلات الأخرى المستخدمة.

يتصل المتحكم بكل من المبدلين S1 وS2 بينما يتصل مع المبدل S3 بشكل غير مباشر عبر المبدل S1.



الشكل(1) طبولوجيا الشبكة المستخدمة

ملخص السيناريوهين المستخدمين هنا:

1. H1 وH5 يمثلان قناة تبادل بيانات عبر بروتوكول TCP، والمهاجم الذي قد يكون H2 أو H3 أو الاثنين معاً.
2. 5 مستخدمين، مستخدم H1 وH5 يمثلان قناة تبادل البيانات ببروتوكول TCP، أحد الأجهزة H2 أو H3 مع H4 يمثلان قناة الاتصال وتبادل البيانات باستخدام بروتوكول UDP، بينما يمثل المهاجم أحد الأجهزة الأخرى H2 أو H3.

سيتم دراسة نتائج تقييم خوارزميات تعلم الآلة في كلا السيناريوهين.

4- أهداف البحث:

يهدف البحث إلى تقييم استخدام آليات تعليم الآلة في كشف هجوم LDoS الذي يؤدي إلى شل وصلة عنق الزجاجة وتقليل جودة الخدمة في بيئة الشبكات المعرفة برمجياً SDN.

5- أهمية البحث:

تأتي أهمية البحث من خلال النقاط الآتية:

- تركز معظم الدراسات بشكل عام على كشف هجمات حجب الخدمة ذات المعدل العالي DoS، وقلة من الدراسات التي تستهدف كشف هجمات LDoS بالرغم من الخطورة التي يسببها هذا الهجوم والذي لايقل أهمية عن الهجوم ذي المعدل العالي.
- أهمية الشبكات المعرَّفة برمجيا SDN كتقنية شبكية حديثة تساهم في تحسين البنى التحتية والنمو السريع للخدمات والتطبيقات الموجودة.
- أهمية تقنيات تعليم الآلة في البحث في التدفقات وكشف الحركية الشاذة للهجوم بناء على مراقبة مجموعة من الميزات الوثيقة بالهجوم بدقة عالية.

6- طرائق البحث ومواده:

من أجل تقييم أداء خوارزميات التعلم الآلي في شبكات SDN: Software Defined Network في كشف هجوم حجب الخدمة منخفض معدل النقل LDoS: Low-Rate Denial of Service، استخدمنا محاكي الشبكات Mininet [18]، والذي يمكن عبره إنشاء شبكة من الأجهزة الافتراضية، المبدلات، المتحكمات والوصلات.

تؤمّن أجهزة Mininet برامج Linux الشبكية الأساسية، وتدعم مبدلاته بروتوكول OpenFlow وهو معيار في الشبكات المعرفة بالبرمجيات SDN، حيث يحدد هذا البروتوكول الاتصال بين المتحكم ومبدلات الشبكة.

بهدف تقييم العمل درسنا عدة بارامترات لقياس الأداء [23, 7] وهي:

1. **خطأ إيجابي FP False Positive**: يسمى خطأ من النوع 1، ويشير إلى إيجاب توقع حصول الحدث وهذا خطأ فالحدث لم يحدث فعلياً، مثلاً: توقع النموذج أن الهجوم حدث ولكنه في الواقع لم يحدث.
2. **خطأ سلبي FN False Negative:** ويسمى خطأ من النوع 2، ويشير إلى نفي حصول الحدث وهذا خطأ فالحدث حصل فعلياً، مثلا: توقع النموذج أن الهجوم لم يحدث ولكنه في الواقع حدث.
3. **FPR False Positive Ratio**: يشير الى نسبة الخطأ الإيجابي بالنسبة الى القيم السلبية الفعلية، ويعطى بالعلاقة التالية:

$$FPR(False\ Positive\ Ratio) = \frac{FP(False\ Positive)}{FP(False\ Positive) + TN(True\ Negative)}$$

4. **FNR False Negative Ratio**: يشير الى نسبة الخطأ السلبي الى القيم الإيجابية الفعلية، ويعطى بالعلاقة التالية:

$$FNR(False\ Negative\ Ratio) = \frac{FN(False\ Negative)}{TP(True\ Positive) + FN(False\ Negative)}$$

5. **الدقة Accuracy**: تشير إلى نسبة عدد التوقعات الصحيحة مقابل عدد التوقعات الكلية وتعطى بالعلاقة التالية:

$$Accuracy = \frac{Number\ of\ Correct\ predictions}{Total\ number\ of\ predictions\ made}$$

6. **Precision:** مقياس أداء يشير إلى عدد التوقعات الموجبة فعلياً من بين التوقعات الإيجابية، ويعطى بالعلاقة التالية: Precision = عدد القيم الإيجابية الحقيقية \ (عدد القيم الإيجابية الحقيقية + عدد القيم التي تمثل خطأ إيجابي)

$$Precision = \frac{TP\ (True\ Positive)}{TP(True\ Positive) + FP(False\ Positive)}$$

7. **Recall:** يسمى هذا المقياس أيضا بالحساسية أو بالمعدل الإيجابي الحقيقي TPR: True Positive Ratio، ويشير إلى عدد التوقعات الموجبة التي توقعها النموذج بشكل صحيح على أنها صحيحة، ويعطى بالعلاقة التالية:

$$Recall = \frac{TP(True\ Positive)}{TP(True\ Positive) + FN(False\ Negative)}$$

8. **F1-Score:** مقياس أداء يجمع بين Precision وRecall، وهي الوسيلة التوافقية للدقة والاسترجاع، ويعرف بالعلاقة التالية:

$$F1\ Score = 2 * \frac{Precision.Recall}{Precision\ + Recall}$$

7- الإطار النظري والدراسات السابقة

7.1 - الإطار النظري:

كما أوردنا سابقاً فإنه يمكن للتعلم الآلي أن يجعل تحقيق الأمن السيبراني أكثر تفاعلية، وفاعلية، وأقل تكلفة. لذا ظهرت العديد من خوارزميات التعلم الآلي التي هدفت إلى كشف هجوم LDoS ولكن باعتماد طرائق مختلفة وميزات مختلفة.

7.2 - الدراسات المرجعية:

1. الدراسة [13] قارنت بين عدة خوارزميات تعلم آلي واعتمدت الشبكة العصبية للانتشار الخلفي (BP Back Propagation) لتحقيقها أعلى دقة كشف، وباستخراج عنصرين بالاعتماد على جدول التدفق من تدفقات الشبكة لاكتشاف هجوم LDoS في شبكات SDN، أظهرت نتائج الاختبار أن هذه الطريقة قدمت تحسيناً على احتمالية الكشف وتخفيضاً للإيجابيات الخاطئة FP، ونتائج التقييم كانت كالآتي:

Accuracy = 98.9%, Precision = 98.17%, Recall = 97.94% and F1 = 98.12%

2. الدراسة [02] قامت بدراسة تأثير هجوم التقليل من الجودة RoQ: Reduction of Quality في شبكات SDN، درست أيضاً عدة خوارزميات تعلم آلي، وحسبت 3 عناصر من تدفقات الشبكة في تصميم نموذج التعلم الآلي، وكانت نتيجة التقييم الأفضل للخوارزمية MLP: Multilayer Perceptron، بالقيم الآتية:

قيمة Precision في كشف تدفقات الهجوم كانت بنسبة 100% و98.62% في كشف التدفقات الطبيعية.

قيمة Recall 96.15% في كشف تدفقات الهجوم و100% في كشف التدفقات الطبيعية.

قيمة F1 98.04% في كشف تدفقات الهجوم و99.30% في كشف التدفقات الطبيعية.

3. أما في الدراسة [11] فلم تستخدم أي من خوارزميات التعلم الآلي، حيث قدمت طريقة حل تستند على الSDN للتخفيف وكشف هجمات LDoS وسميت بـ SoftGuard، إذ يكتشف الهجوم عن طريق تثبيت قواعد تدفق مسبقة في جداول تدفق المبدلات، لمراقبة تدهور إجمالي إنتاجية TCP على المنافذ، وتخفيف الهجوم يتم بعد تحديد المهاجم عبر مراقبة الزيادة في التدفق وعلى أي منفذ فيتم خنق تدفقات الهجوم عبر حد عرض الحزمة أو إسقاطها، نتائج الأداء كالتالي:

Accuracy ~= 90%, FNR = 6%, FPR = 4%

الدراسات التالية قامت بالبحث في كشف هجمات LDoS في الشبكات التقليدية اعتماداً على خوارزمية تعلم آلي:

4. كما في الدراسة [9] باستخدام خوارزمية تعلم آلي AdaBoost في كشف هجمات LDoS ولكن في الشبكات التقليدية، واستخرجت حتى 13 عنصر لتدريب واختبار نموذج التعلم الآلي، وكانت النتائج المحققة كالتالي:

Accuracy = 97.06%, FNR = 2.94% and FPR = 0.33%

5. الدراسة [8] اقترحت استخدام خوارزمية تعلم آلي دون اشراف وهي خوارزمية BIRCH، واعتمدت على عنصرين في تدريب واختبار النموذج الآلي، فكانت النتائج كالتالي:

FPR = 0.75%, FNR = 0%, Accuracy = 99.2%, Precision = 98.16%, Recall = 100%, F1 = 99%

6. بينما اعتمدت الدراسة [12] على خوارزمية Logistic Regression المحسّنة في كشف الهجوم واستخلاص 4 عناصر لتدريب واختبار نموذج التعلم الآلي، وكانت النتائج كالتالي:

FPR = 0.38%, FNR = 0.42%, Accuracy = 99.58%

7. قامت الدراسة [014] باستخدام الخوارزمية Isolation Tree في كشف الهجمات LDoS، بالاعتماد على 3 عناصر، وكانت نتائج التقييم كالتالي:

FPR = 0.13%, FNR =0%, Accuracy = 100%

8. الدراسة [6] استخدمت KNN والاعتماد على 3 عناصر، والنتائج كانت كالتالي:

Accuracy = 99.22%, FNR = 0.78%, FPR = 0.33%

9. الدراسة [10] استخدمت الخلايا العصبونية الملتفة CNN Convolutional neural network في كشف هجمات LDoS في شبكات SDN، والاعتماد على 17 عنصر، والنتائج كانت كالتالي:

Accuracy = 97.1%, FNR = 2.9%, FPR = 0%

10. الدراسة [15] استخدمت خوارزمية SVM: Support Vector Machine مع 3 عناصر، ونتائج الأداء كانت كالتالي:

Accuracy = 98.41%, FNR = 1.59%, FPR = 6.21%

8- عملية اختيار العناصر الأكثر ارتباطاً مع الهجوم ومخططاتها:

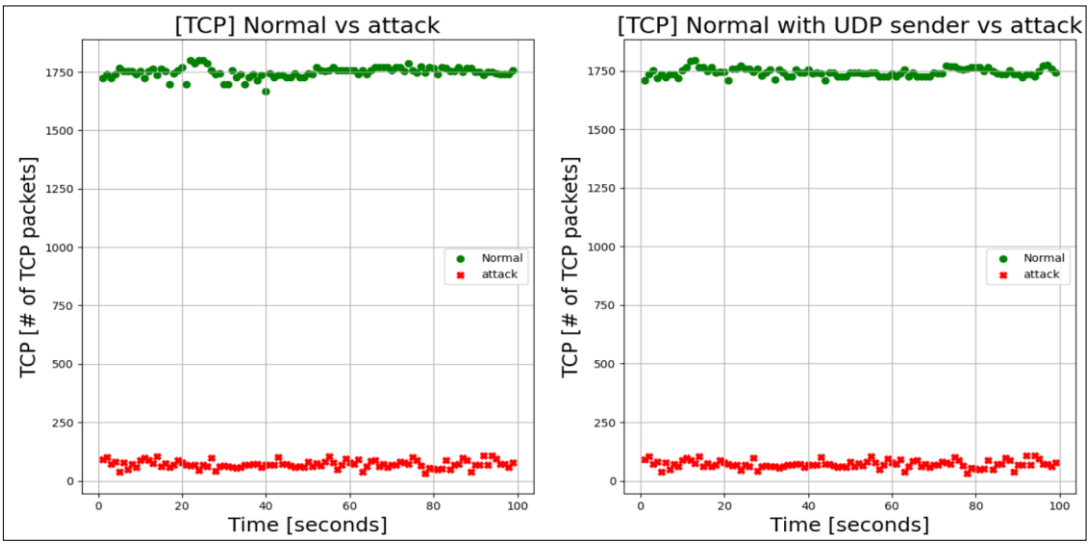
ستعرض المخططات الآتية العناصر الأكثر ارتباطاً بهجوم LDoS في كلا السيناريوهين (وجود قناة اتصال TCP ومستخدمUDP طبيعي وعدم وجود مستخدم UDP أبداً وفي الحالتين يوجد مهاجم).

هجوم LDoS يعتمد بشكل أساسي على رزم UDP والمتأثر الأساسي هو آليات التحكم بالازدحام الخاصة ببروتوكول TCP، لذلك فالتغييرات التي تحصل تشمل كل من قيم رزم TCP وUDP، وبالتالي بدراسة هذه القيم والتغييرات الإحصائية التي تطرأ عليها فإننا نأمل إيجاد نمط فريد تسلكه تدفقات الشبكة في كل سيناريو يمكّن نموذج التعلم الآلي من التمييز في المستقبل تلقائياً والتصنيف بوجود هجوم من عدمه، ومنه اعتمد العناصر والرسوم البيانية الآتية علماً أن:

النقطة باللون الأخضر والشكل الدائري تمثل الحالة الطبيعية، بينما النقطة باللون الأحمر وشكل x تمثل حالة الهجوم.

من خلال التجربة وجدنا تفاوت بين العديد من العناصر في إمكانية إيجاد نمط واضح للتمييز بين حالتي وجود الهجوم من عدمه في كلا السيناريوهين، ومن المؤشرات التي تعطي نمطاً واضحاً، وبذلك نتائج تقييم أفضل وتعقيد أقل وسرعة في التدريب، وهذه العناصر هي: عدد رزم TCP، الانحراف المعياري لرزم UDP، الانحراف لرزم TCP وUDP، نسبة UTR: UDP TCP Ratio، لذلك ستعتمد في تعليم نموذج التعلم الآلي لتصنيف وجود الهجوم من عدمه.

1. **عدد رزم TCP**: تمثل عدد الرزم في كل واحدة زمن (زمن التقرير) لرزم TCP، نستدل منه على إمكانية التمييز بين حالتي وجود الهجوم من عدمه في السيناريوهين المستخدمين، حيث نلاحظ في الشكل(2) أن عدد رزم TCP فوق مقدار محدد (1500 رزمة) يدل على الحالة الطبيعية في السيناريوهين، بينما عدد رزم TCP أقل من 250 رزمة في الثانية تدل على حالة وجود هجوم (نتيجة الهجوم يقل معدل رزم الـ TCP)، ومنه نلاحظ حصول تغيير واضح يحصل في كل حالة وكل سيناريو أي يمكن اعتماد هذا العنصر كمؤشر لتعليم النموذج الآلي للتمييز بين حالة وجود الهجوم من عدمه.

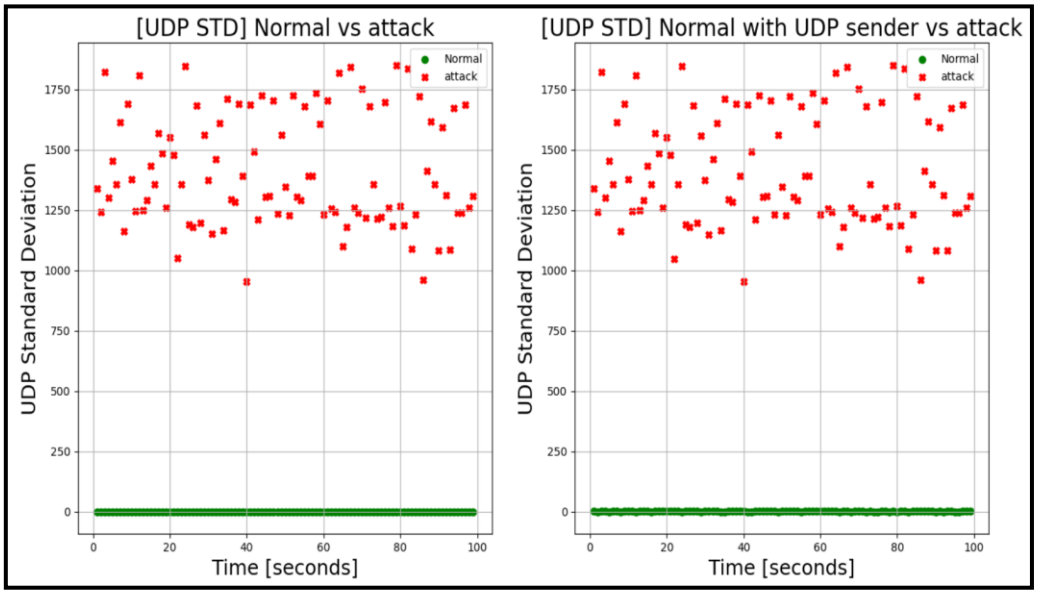


الشكل (2) مخطط TCP مقابل الزمن لكل من السيناريوهين

2. **الانحراف المعياري لرزم UDP**: يشير إلى مدى التشتت داخل مجموعة البيانات، ويقاس رياضياً عبر أخذ الجذر التربيعي لقيمة الـ Variance، وهو مدى الانتشار والابتعاد عن قيمة المتوسط الحسابي.

$$Standard\ Diviation\ STD = \sqrt{Variance} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2}$$

تحقق قيمة الانحراف المعياري لرزم الـ UDP كما في الشكل (3) توزعاً يوضّح التباين بين حالتي وجود الهجوم من عدمه في السيناريوهين، وهذا يعطينا مؤشراً آخر لتعليم النموذج الآلي للتمييز بين حالتي حدوث الهجوم من عدمه.

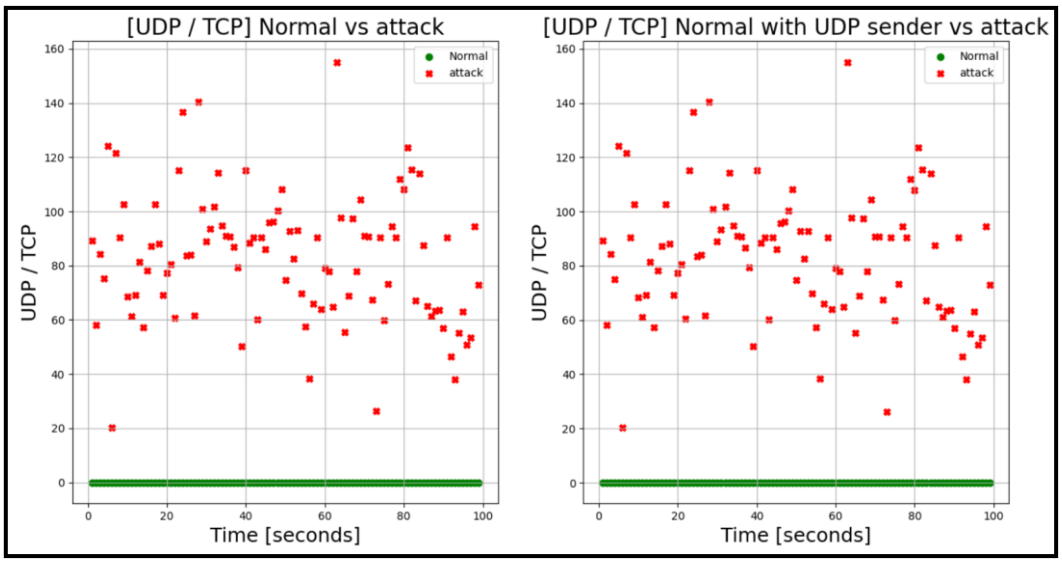


الشكل (3) مخطط الانحراف المعياري لـ UDP مقابل الزمن لكل من السيناريوهين

3. **نسبة عدد رزم UDP إلى عدد رزم TCP:**

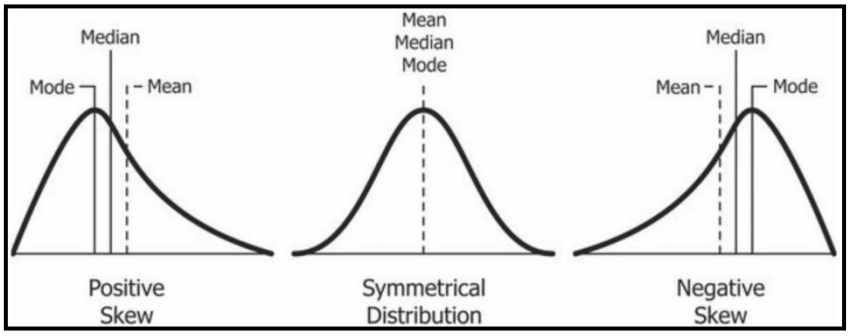
مؤشر إضافي للتفريق بين حالتي وجود الهجوم من عدمه، يشير إلى نسبة عدد رزم UDP إلى عدد رزم TCP.

إن عدد رزم الـ TCP الكبير في الحالة الطبيعية في المقام يعطي نسبة UTR صغيرة جداً، بينما في حالة حصول الهجوم وبسبب تناقص عدد رزم الـ TCP ستزداد قيمة النسبة السابقة، وبالنتيجة ستتغير قيم الـ UTR بشكل كبير عند حصول الهجوم، ويظهر الفرق في الحالتين في الشكل (4) الآتي:



الشكل (4) مخطط UTR مقابل الزمن لكل من السيناريوهين

4. **الانحراف Skewness**: من مقاييس الشكل، وهو مقياس لعدم تماثل التوزيع [29, 33, 30]، يخبرنا التباين عن مقدار التباعد عن المتوسط بينما يعطي الانحراف اتجاه التباين، ويظهر الانحراف في عدة أشكال كما في الشكل (5)، ويقسم إلى انحراف سلبي وإيجابي أو دون انحراف (توزيع متناظر):



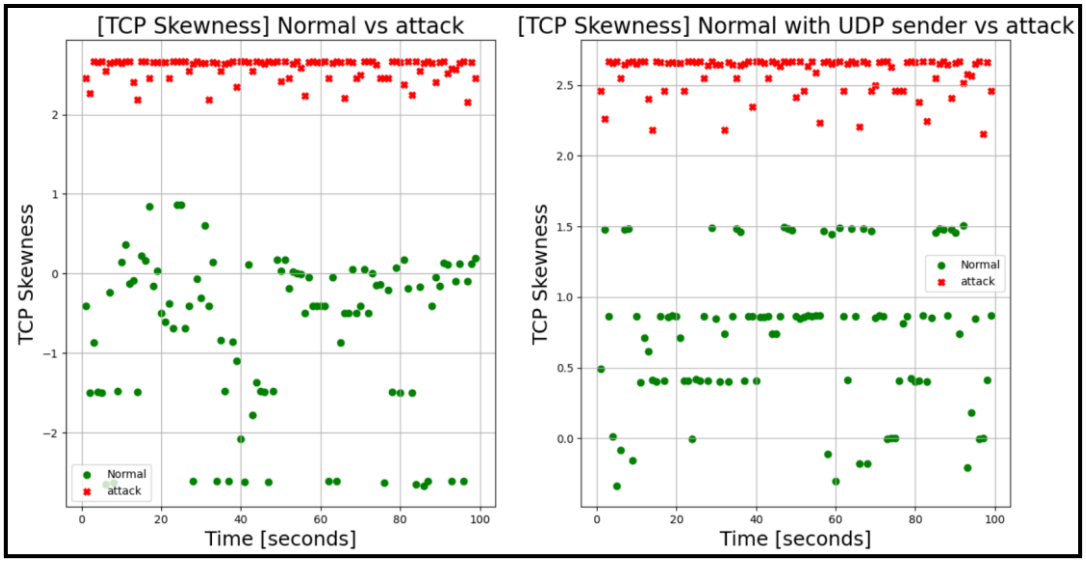
الشكل (5) حالات الانحراف

رياضيا يحسب كالآتي:

$$;Mode = 3\,(\,Median\,) - 2\,(Mean) \rightarrow Skewness = \frac{(\,Mean - Mode\,)}{Standard\ Deviation}$$

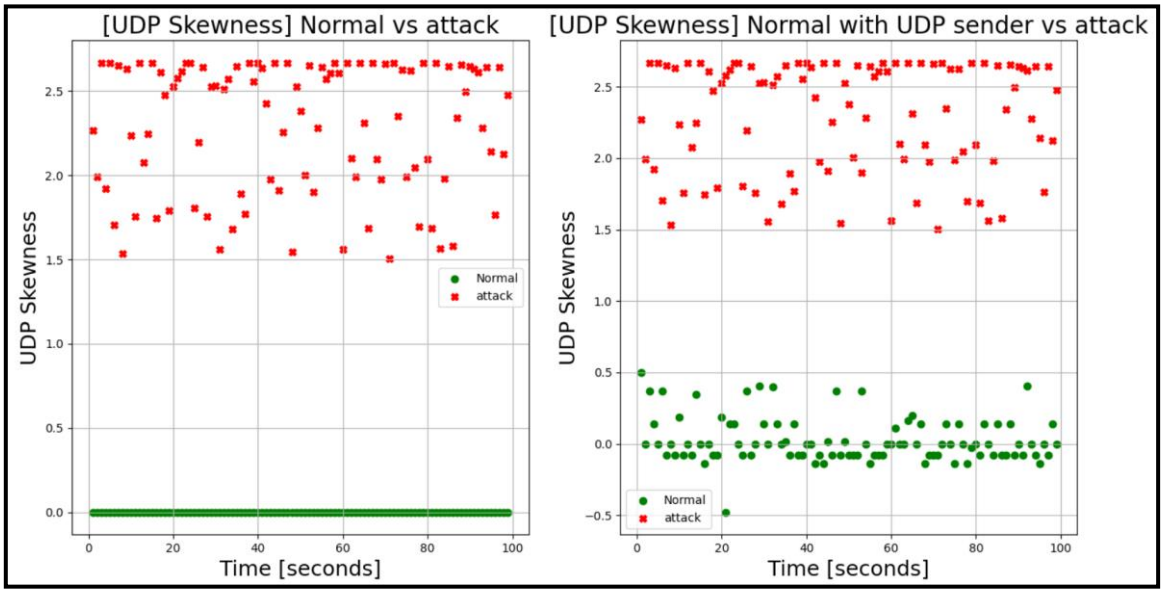
$$Skewness = 3\frac{(\,Mean - Median\,)}{Standard\ Deviation}$$

إن مقياس الانحراف الشكلي يعطي انطباع عن اتجاه التباين لرزم TCP، فكما يظهر في الشكل (6) نجد أنه من السهل على نموذج التعلم الآلي أن يجد نمط يحدد من خلاله حالة وجود الهجوم من عدمه في حالة السيناريوهين حيث توزعت القيم لحالة وجود الهجوم فوق قيمة 2.



الشكل (6) مخطط انحراف TCP مقابل الزمن لكل من السيناريوهين

واستخدام مؤشر الانحراف لرزم UDP كما يظهر في الشكل (7) يبين تمييز واضح بين حالتي وجود الهجوم من عدمه، ويمكن لنموذج التعلم الآلي التفريق بسهولة بين حالتي وجود الهجوم من عدمه في السيناريوهين.



الشكل (7) مخطط انحراف UDP مقابل الزمن لكل من السيناريوهين

9- بعض خوارزميات التعلم الآلي المستخدمة:

1. الانحدار اللوجستي Logistic Regression

إحدى خوارزميات التعلم الآلي الخاضع للإشراف المخصصة لمهام "التصنيف"، والفائدة الأساسية للانحدار اللوجيستي هو الحصول على قيمة خرج احتمالية (تقع بين 0 و1)، مناسب لمشاكل التصنيف إلى فئتين ويمكن تعميمه إلى فئات متعددة [3].

2. خوارزمية k الجار الأقرب KNN:

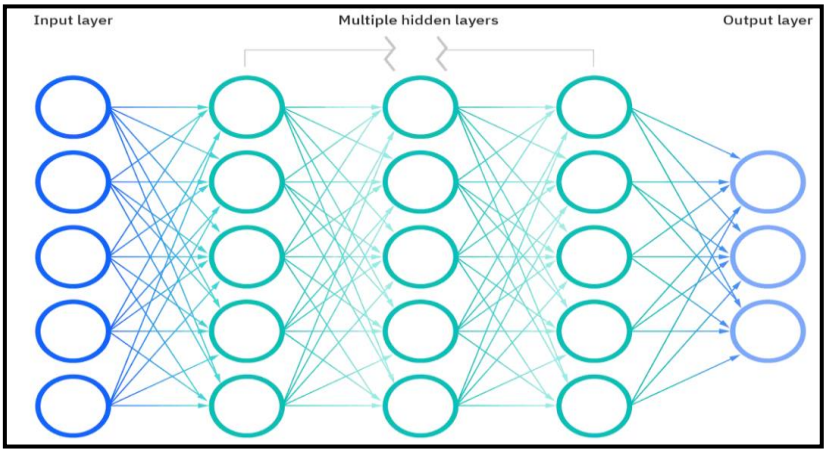
خوارزمية k الجار الأقرب (KNN) هي نوع بسيط من خوارزمية التعلم الخاضع للإشراف المستخدمة لكل من التوقع والتصنيف.

تعمل بآلية حساب المسافة بين النقطة المراد تصنيفها والنقاط بعدد k الأقرب لها (عادة ما يستخدم مقياس المسافة الإقليدية)، ثم اعتبار النقطة تتبع للمجموعة ذات عدد النقط الأكبر والأقرب إلى النقطة المراد تصنيفها [1, 25].

3. الشبكات العصبونية Neural Networks:

تعد إحدى خوارزميات التعلم الآلي **الخاضع للإشراف** التي تعكس سلوك الدماغ البشري، مما يسمح لبرامج الكمبيوتر بالتعرف على الأنماط وحل المشكلات الشائعة في مجالات الذكاء الاصطناعي والتعلم الآلي والتعلم العميق، هي مجموعة فرعية من التعلم الآلي وتقع في قلب خوارزميات التعلم العميق.

تتكون الشبكات العصبونية الاصطناعية من طبقات مؤلفة من عقد، تتكون الشبكة من طبقة إدخال، وطبقة مخفية واحدة أو أكثر، وطبقة إخراج. كل عقدة أو خلية عصبية اصطناعية تتصل بأخرى ولها وزن وعتبة مرتبطة بها. إذا كان ناتج أية عقدة فردية أعلى من قيمة العتبة المحددة، تنشط تلك العقدة، وترسل البيانات إلى الطبقة التالية من الشبكة. وبخلاف ذلك، لن يتم تمرير أية بيانات إلى الطبقة التالية من الشبكة [31, 27]، كما في الشكل (8):



الشكل (8) شبكة عصبونية

4. خوارزمية BIRCH:

هي خوارزمية **تعلم دون إشراف**، وهي اختصار لـ (Balanced Iterative Reducing and Clustering using Hierarchies)

تستخدم بشكل أساسي من أجل تقسيم مجموع البيانات الكبيرة إلى عناقيد للخوارزمية 4 مراحل، ولكن باستخدام المرحلتين الأهم يمكن تسميتها أيضاً التقسيم إلى عناقيد بخطوتين Two-Step Clustering، حيث تبدأ المرحلتان بتقسيم البيانات باستخدام هيكل شجري إلى مجموعة عناقيد صغيرة، ثم تطبق خوارزميات تجميع في عناقيد مثل خوارزمية Agglomerative Clustering التجميع الهرمي على العناقيد الأصغر التي تشكلت في التجميع الأول، وهذا يوفر عناء التجميع المباشر لكامل مجموعة البيانات إلى عناقيد، لذلك فهي تناسب مجموعة البيانات الكبيرة جداً، وطورت هذه الخوارزمية في 1996 من قبل Tian Zhang, Raghu Ramakrishnan, and Miron Livny [16, 20].

10-المعالجة المسبقة وهندسة العناصر:

التقييس (توحيد المجالات) وتنظيف البيانات:

يسبّب التفاوت في مجالات القيم بين العناصر التي تم حسابها انحياز في التدريب نحو البيانات ذات المجالات الأكبر لذلك قمنا بتقييس rescaling مجموعة البيانات في مجال قياس واحد بحيث تكون قيمة الانحراف المعياري والتباعد تساوي 1 عبر القيام بعملية Standardization.

والتي تعتمد العلاقة الآتية: $x_{new} = \frac{x-\mu}{\sigma}$ (μ تمثل المتوسط الحسابي، σ تمثل الانحراف المعياري).

تنظيف البيانات يشمل إزالة القيم الصفرية، الفارغة وإزالة أي قيم لانهائية أو أي قيم قد تسبب فشل في عملية خوارزمية التعلم.

ضبط قيم البارمترات في خوارزميات تعلم الآلة المستخدمة:

تم استخدام الصنف GridSearchCV [24] الذي يبحث ويحسب أداء الخوارزمية في حالة استخدام كل البارامترات التي تقدم لها ثم اختيار البارامترات الأفضل التي تعطي نتيجة التقييم الأفضل، حيث اختبرت كل خوارزمية تعلم آلي بمختلف البارامترات التي تدعمها ثم اعتمدت البارامترات النهائية التي أعطت أفضل قيم دقة.

11-خوارزميات التعلم الآلي المستخدمة:

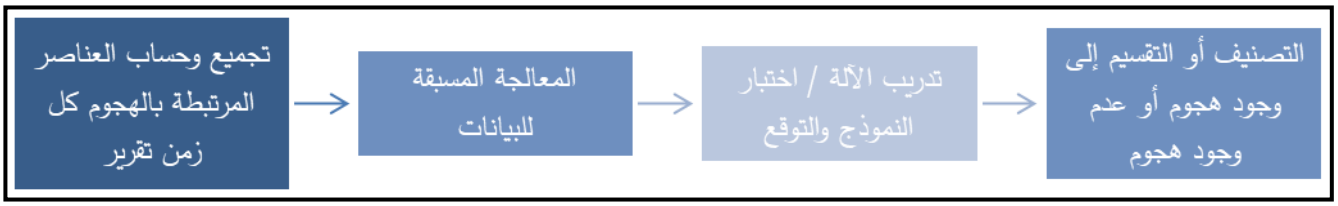
يوجد حالتي تصنيف إما يوجد هجوم أو لا يوجد هجوم، وبذلك يعتبر التصنيف ثنائياً، سيتم اختبار مجموعة خوارزميات ومصنفات تعلم آلي وهي الخوارزميات الـ 4 الآتية:

Logistic regression, Neural Network, K-Nearest Neighbor and BIRCH (Two-Step Clustering).

تدعم مكتبة Scikit Learn هذه الخوارزميات الأربعة [28, 26, 21, 22] ولكل منها عدد من البارامترات التي تلعب دوراً هاماً في نتائج تقييم النموذج النهائي.

12- المخطط الصندوقي النهائي للكشف:

خوارزمية العمل عملياً:



13-التطبيق العملي:

تمت بالتزامن مع تشغيل المتحكم والشبكة في بيئة ubuntu، ومواصفات الجهاز مضيف المحاكي هي كالآتي:

1- وحدة معالجة مركزية:

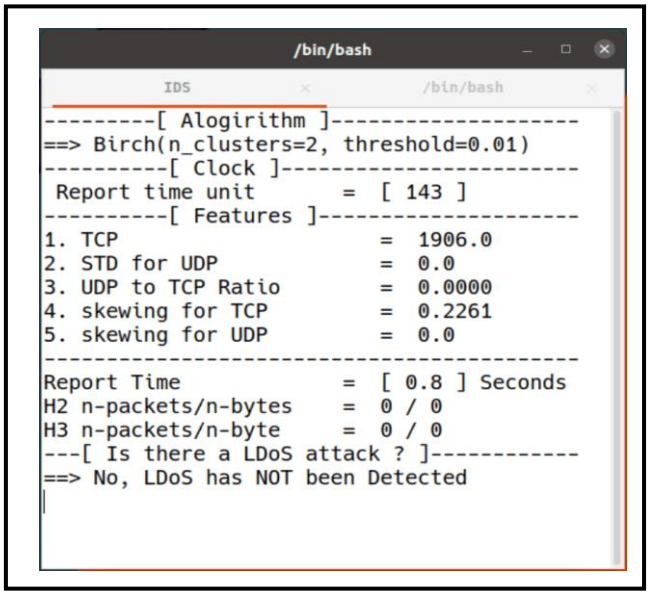
AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx, 2100 MHz, 4 Core(s), 8 Logical Processor(s).

2- ذاكرة عشوائية: 8 [غيغا بايت].

وتظهر الواجهة لكل نافذة طرفية قيم العناصر المختارة كل واحدة زمن تقرير وعليه يتم تنفيذ النموذج المدرب سابقاً ليتنبأ بالقيمة الناتجة (وجود هجوم أو حالة طبيعية).

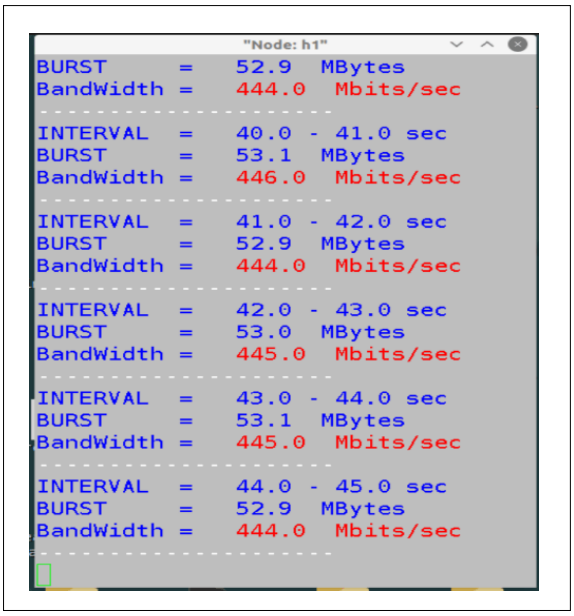
الخطوات كالآتي: يتم تشغيل المتحكم Ryu، ثم يتم تشغيل المحاكي Mininet.

وفي نافذة طرفية إضافية يتم تشغيل الكود المسؤول عن الكشف IDS.py بالواجهة كما في الشكل (9)، يدرب هذا البرنامج الآلة على ملف csv. المنشأ مسبقاً من خلال تجميع حركة المرور وحساب العناصر التي تم اختيارها سابقاً ثم توقع الناتج كل زمن تقرير.



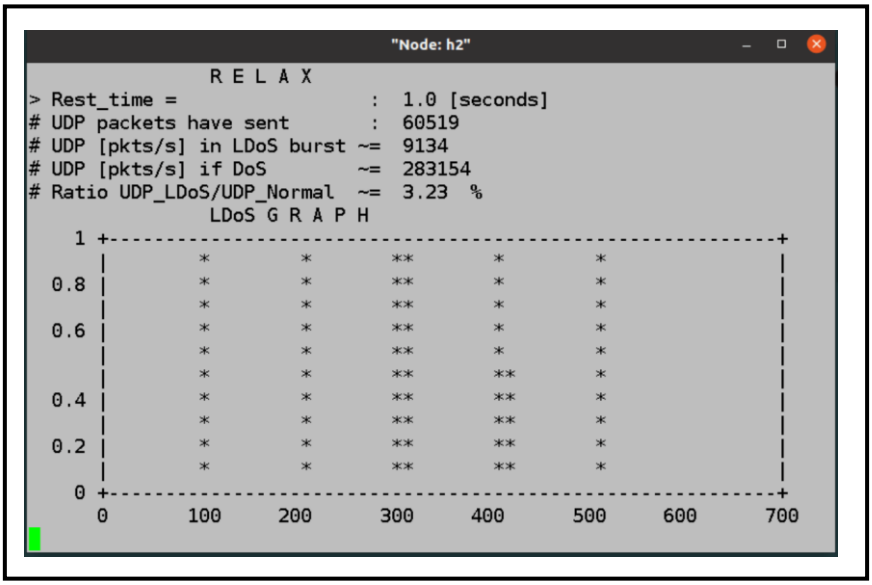
الشكل (9) تشغيل برنامج IDS لكشف الهجمات فقط كما يظهر في الصورة السابقة الحالة

تظهر الإنتاجية في تقرير أداة IPERF كما في الشكل (10):



الشكل (10) النافذة الطرفية للمستخدم H1 وتُظهر قيمة الإنتاجية في كل زمن تقرير

نافذة المهاجم تظهر كما في الشكل (11):

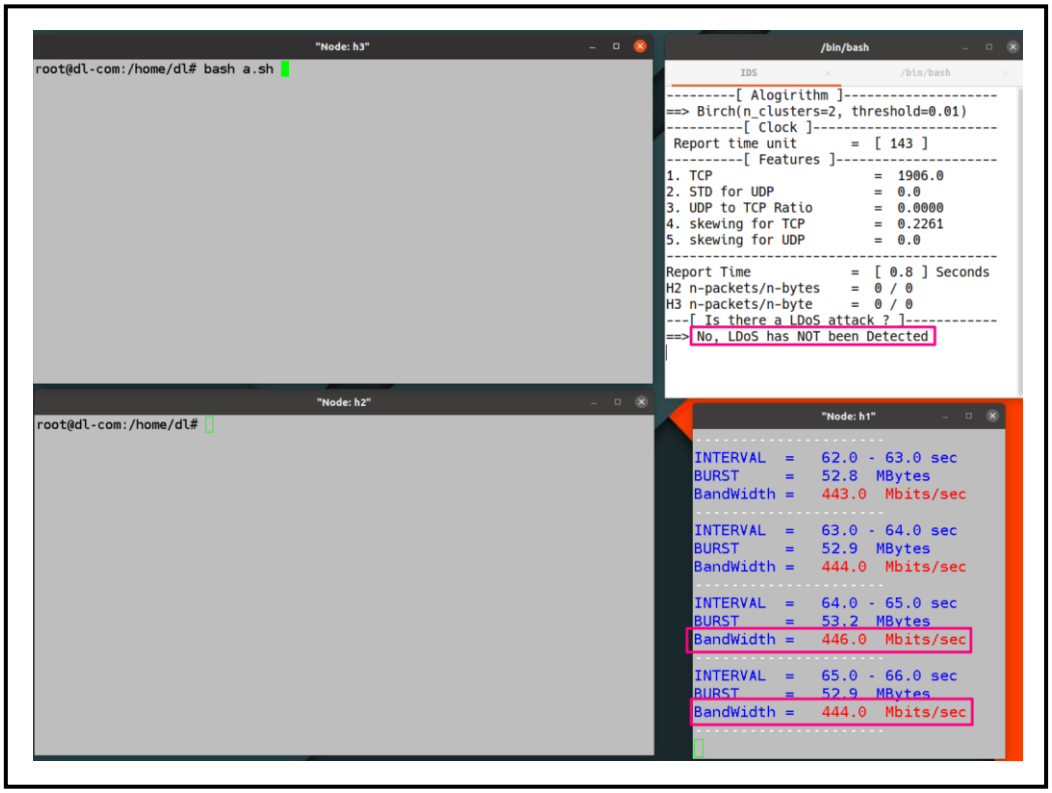


الشكل (11) نافذة المستخدم H2 عندما يعمل كمهاجم

1- السيناريو الأول:

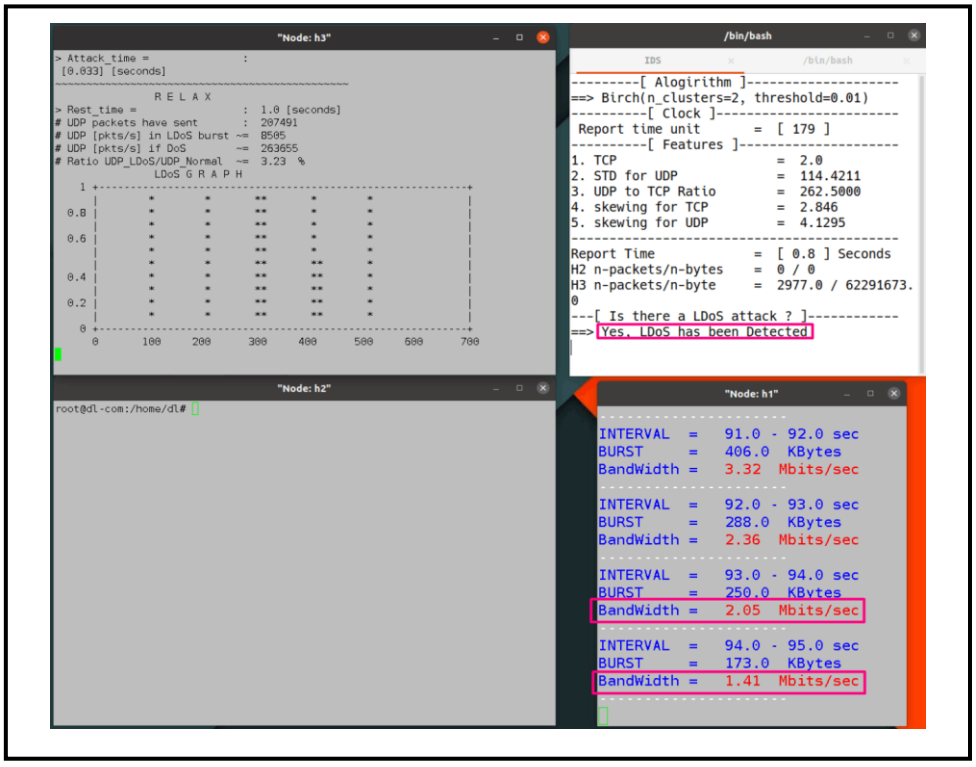
في السيناريو الأول يوجد مهاجم ومستخدم شرعي يعمل ببروتوكول نقل TCP فقط.

يظهر الشكل (12) مجموعة نوافذ طرفية تشير كل منها إلى جهاز، حيث يوجد قناة اتصال بنمط TCP بين H1 وH5 ونلاحظ أن نتيجة الكشف هي طبيعية وذلك لأنه لا يوجد أي مهاجم حتى الآن.



الشكل (12) الحالة الطبيعية لعمل الشبكة

بدأ H3 الهجوم وخلال واحدة زمن التقرير اكتشف وجود الهجوم وتغيرت نتيجة التقرير، كما يبين الشكل (13)، ويعرض مؤشر الإنتاجية انخفاضاً كبيراً يظهر في نافذة H1.

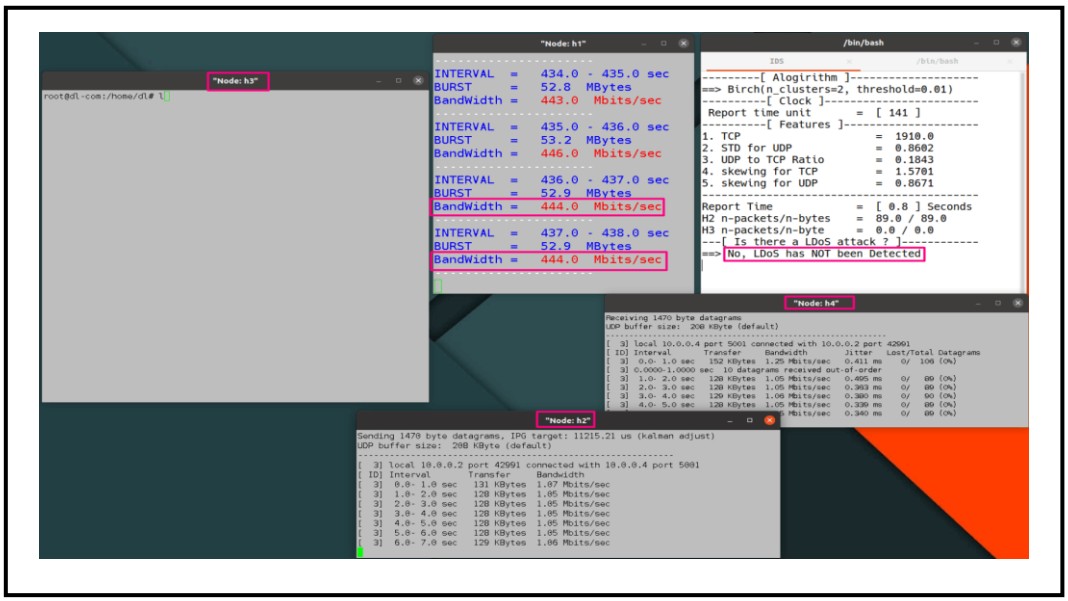


الشكل (13) حالة وجود مهاجم (H3)

2- السيناريو الثاني:

في السيناريو الثاني يوجد مهاجم ومستخدم شرعي يعمل ببروتوكول نقل TCP ومستخدم شرعي آخر يعمل ببروتوكول UDP.

يعرض الشكل (14) قناة تبادل بيانات بين H2 وH4 باستخدام بروتوكول النقل UDP، بالإضافة إلى وجود المستخدم H1 والذي يتواصل مع H5 باستخدام بروتوكول TCP، وحالة الشبكة في الوضع الطبيعي وهذا ما يظهره تقرير الكشف أيضا وذلك لعدم وجود أي مهاجم حتى الآن.



الشكل (14) حالة وجود مستخدم UDP

بدأ H3 الهجوم وخلال واحدة زمن التقرير اكتُشف وجود الهجوم وتغيرت نتيجة التقرير كما يظهر في الشكل (15)، ويعرض مؤشر الإنتاجية انخفاضاً يظهر في نافذة H1، نلاحظ قدرة نموذج التعلم الآلي في كشف الهجوم حتى في حالة وجود مستخدم آخر يستخدم بروتوكول النقل UDP وهو نفس البروتوكول الذي يستخدمه المهاجم.

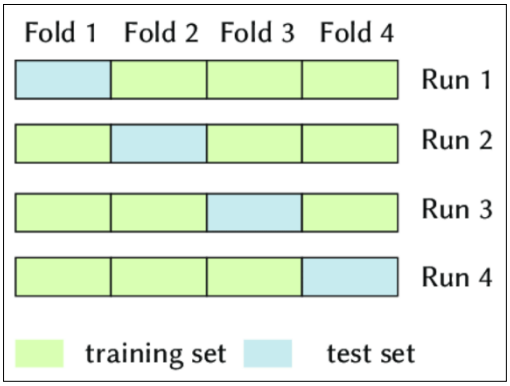
الشكل (15) حالة وجود هجوم مع مستخدم UDP

13.1- التقييم وجدول القيم التي حصلنا عليها لكل خوارزمية مستخدمة:

تقييم خوارزميات التعلم الآلي يتم على أساس بيانات جديدة لم تراها الخوارزمية سابقاً، لذلك ستقسم مجموعة البيانات إلى مجموعة تعليم Train Set ومجموعة تدريبTest Set، تقدم مكتبة Scikit Learn مجموعة آليات للتقسيم وسيتم اختيار الآلية KFold [32, 19].

وذلك لكون هذه العملية تعمل على تقسيم مجموعة البيانات إلى مجموعات جزئية بعدد k، يتعلم النموذج على k-1 قسم، ثم يتم اختبار النموذج بالقسم الباقي (يعتبر بيانات جديدة وبالتالي ملائم لاستخدامه كبيانات اختبار)، تحفظ النتيجة ثم يدرَّب النموذج مجدداً على k-1 الأقسام التالية.

يقدم الشكل (16) مثالاً توضيحياً لآلية تقسيم مجموعة البيانات باستخدام KFold:

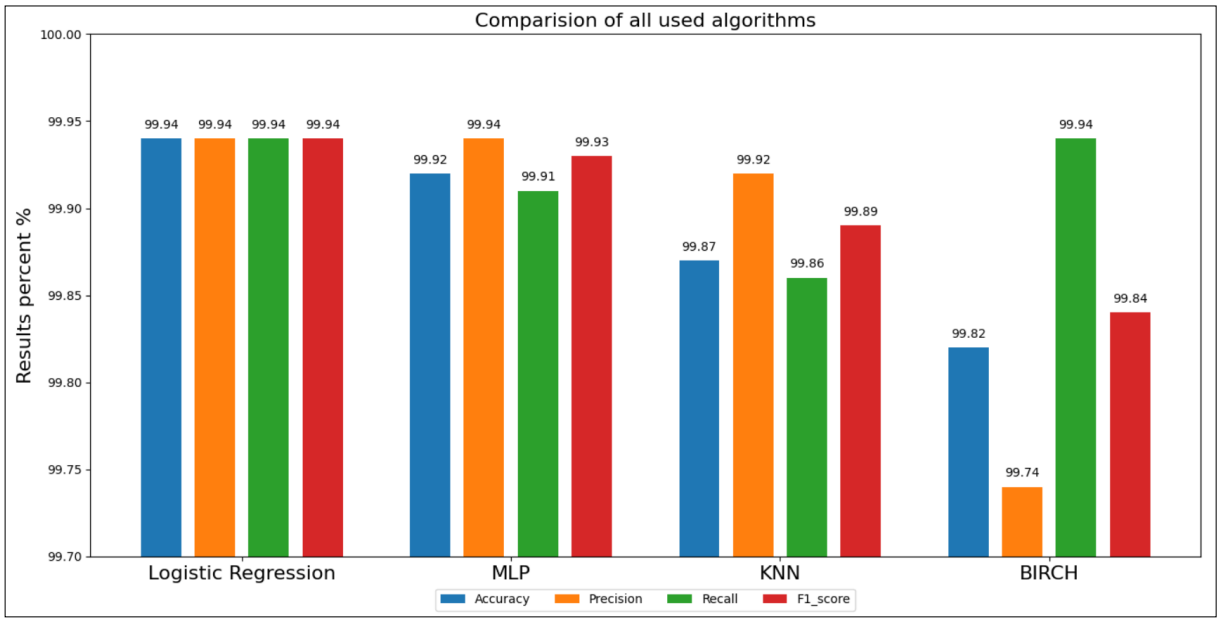


الشكل (16) يمثل آلية عمل KFold

قسمت مجموعة البيانات كما في الشكل (16) السابق إلى 4 أقسام متساوية، بمعنى اختيرت قيمة، k=4 ويبدأ حساب أداء خوارزمية التعلم الآلي في مجموعة البيانات من خلال تعليم الآلة على الأقسام الـ 3 واختبار النموذج بالقسم الرابع، بعد ذلك يؤخذ قسم جديد لاعتباره قسم اختبار ويدرب النموذج على الأقسام الأخرى إلى أن يدرب ويختبر النموذج بكل قسم فيؤخذ المتوسط الحسابي لقيم الأداء التي نتجت في التقسيمات الأربعة.

14- النتائج.

أجرينا التقييم باستخدام k = 10، لكل خوارزمية والنتيجة النهائية أخذت كمتوسط حسابي لكل المحاولات، فكانت النتائج متقاربة إلى حد ما وهذا ما يظهر في الشكل (17):



الشكل (17) المقارنة بين خوارزميات التعلم الآلي المستخدمة وكل مقاييس الأداء

بالنسبة لخوارزمية Logistic Regression وسنرمز لها LR فإنها تحقق من ناحية عامل الدقة Accuracy أعلى قيمة بمقدار 99.94% بينما تحقق 99.92، 99.87 و99.82 % في خوارزميات الخلايا العصبية وسنرمز لها MLP (Multilayer perceptron) وKNN وBIRCH على الترتيب.

من ناحية عامل الـ precision نجد أن خوارزمية LR وMLP تتساوى عند قيمة 99.94% بينما تحقق 99.92 و99.74 في كل من KNN وBIRCH على الترتيب.

بالنسبة لعامل Recall فكانت القيمة العليا 99.94% لكل من خوارزميتي LR وBIRCH، بينما 99.91، 99.86 في كل من MLP وKNN على الترتيب.

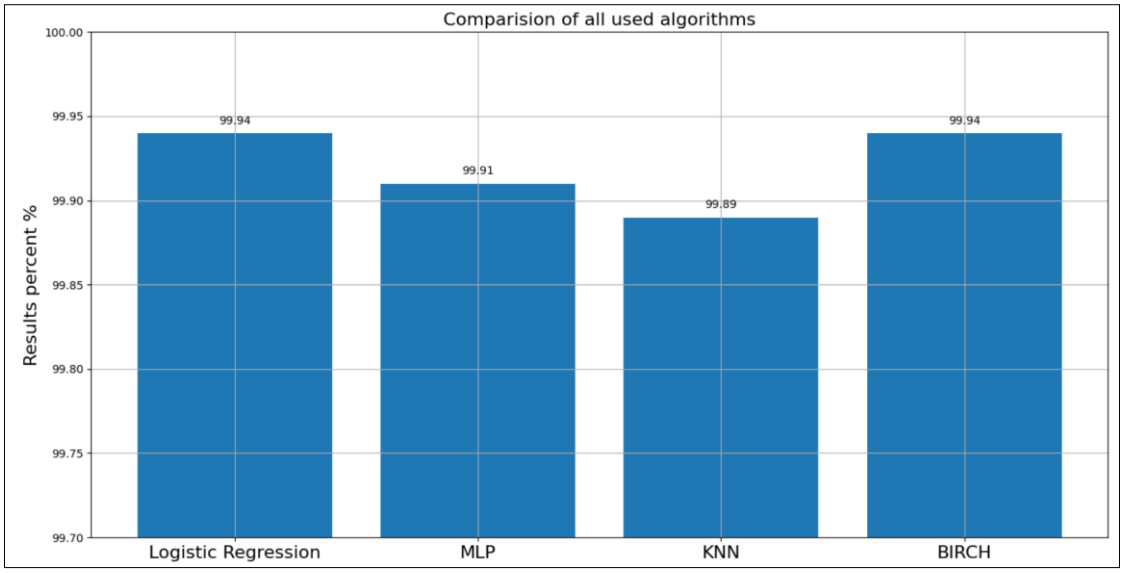
بالنسبة لمقياس التقييم F1_score فكانت القيمة العليا للخوارزمية LR، وحققت الخوارزميات MLP، KNN، BIRCH القيم التالية 99.93، 99.89 و99.84% على الترتيب.

يمكن تفسير تحقيق هذه النتائج المرتفعة بشكل عام بسبب الخطوات المستخدمة في تجهيز البيانات، اختيار العناصر، هندستها وخطوة ضبط البارامترات.

من المهم جداً بما أننا نصمم نظام كشف هجمات إلكترونية الحرص على أن تكون قيمة النفي الكاذب الـ FN: False Negative أقل ما يمكن، فالكلفة الكبيرة التي تحصل نتيجة وجود الهجوم عندما يتوقع النموذج أن الحالة

طبيعية أكبر مما عليه في حالة توقع النموذج وجود الهجوم وفعلياً لا يوجد هجوم وعندها يكفي إجراء اختبارات إضافية بالاعتماد على التقنيين لتأكيد وجود الهجوم والتعامل مع الأمر.

أي أنه في حالة الكشف يهمنا التركيز على أن تكون قيم Recall أكبر مايمكن، لذلك قارنا بين الخوارزميات بمقياس الـ Recall فقط، وهذا ما يظهر في الشكل (18):



الشكل (18) المقارنة بين خوارزميات التعلم الآلي بالنسبة لمقياس Recall

نجد بالترتيب التنازلي أن خوارزميتي LR وBIRCH تعطي قيم متماثلة مرتفعة متماثلة من ناحية Recall وبعدها MLP ثم خوارزمية KNN.

جدول (1) المقارنة في الأداء لكل من خوارزميات التعلم الآلي:

	Accuracy	Precision	Recall	F1-Score
LR	99.94	99.94	99.94	**99.94**
MLP	99.92	99.94	99.91	**99.93**
KNN	99.87	99.92	99.86	**99.89**
BIRCH	99.82	99.74	99.94	**99.84**

من الجدول السابق نجد أن استخدام الخوارزمية BIRCH أو Logistic Regression هو الأنسب.

15- مناقشة النتائج.

ستتم المناقشة بين نتائج كشف هجوم LDoS والنتائج في الدراسات الآتية، من حيث قيم الأداء واستخدام آليات التعلم الآلي، وهل ستستخدم في شبكات SDN أم لا، وزمن الكشف الوسطي، وخوارزميات التعلم الآلي المستخدمة، وهذا ما يظهر في الجدول 2 التالي.

جدول (2) المناقشة بالنسبة لدراسات سابقة.

الدراسة	دقة الكشف %	FNR %	FPR %	SDN	استخدام ML؟ وما هي الخوارزميات المستخدمة	زمن الكشف [ثانية]
[9]	97.06	2.94	0.33	لا	نعم، Adaboost	~3
[8]	98.06	0.61	1.33	لا	نعم، BIRCH	~3
[14]	97.00	3	4.5	لا	نعم، Isolation Forest	~5
[6]	99.22	0.78	0.33	لا	نعم، KNN	~0.05
[10]	97.1	2.9	0	لا	نعم، Convolutional Neural Network	~5
[15]	98.41	1.59	6.21	لا	نعم، SVM	~1
[12]	99.58	0.42	0.38	لا	نعم، Improved Logistic Regression	0.5
[2]	98.9	3.85	0	نعم	نعم، عدة خوارزميات تعلم آلي، حققت MLP: Multilayer Perceptron قيمة أداء أعلى.	-
[13]	99.2	0.7	2.7	نعم	نعم، استخدمت عدة خوارزميات واعتمدت Neural Network لأنها حققت أفضل قيم أداء.	~1.11
[11]	حوالي 90	6	أصغر من 4	نعم	لا	-
دراستنا	99.94	0.05	0.07	نعم	نعم، استخدمت عدة خوارزميات واعتمدت Logistic Regression	~1

كما موضح في الجدول السابق فإن دراستنا حققت نتائج أفضل من حيث دقة الكشف وبزمن كشف حوالي 1 ثانية ومعدل أخطاء صغير FNR 0.05% وFPR يساوي 0.07%.

16- الخلاصة:

مما سبق نستنتج أن هذا البحث قد أعطى النتائج التالية:

1- هجمات LDoS ممكنه وضررها لا يقل أهمية عن هجمات حجب الخدمة ذات المعدل العالي.
2- كشف هجمات LDoS في بيئة شبكات SDN ممكن عبر استخدام خوارزميات التعلم الآلي بدقات كشف متفاوتة.
3- خوارزمية Logistic Regression أعطت دقة كشف أكبر وبمعدل أخطاء إيجابية وسلبية أقل مما لدى الخوارزميات الأخرى في السيناريوهين المستخدمين سابقا، حيث تمكنت الخوارزمية من كشف الهجوم خلال زمن وقدره تقريبا 1 ثانية.

17-التوصيات:

بناءً على النتائج التي تم التوصل إليها نوصي بالتالي:

1- البحث عن خوارزميات تعلم آلي ML أخرى.
2- استخدام النتائج السابقة في البحث عن وسائل للتصدي.
3- التركيز على سرعة الكشف والتصدي قدر الإمكان.

18- قائمة المراجع.

18.1- المراجع الورقية:

[1] Alharbi, Y., Alferaidi, A., Yadav, K., Dhiman, G., & Kautish, S. (2021). Denial-of-service attack detection over ipv6 network based on KNN algorithm. Wireless Communications and Mobile Computing, 2021.

[2] de Miranda Rios, V., Inácio, P. R., Magoni, D., & Freire, M. M. (2021). Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms. Computer Networks, 186, 107792.

[3] Edgar, T., & Manz, D. (2017). Research methods for cyber security. Syngress.

[4] Guo, L., & Lee, J. Y. (2021). TCP-FLASH-A Fast Reacting TCP for Modern Networks. IEEE Access, 9, 68861-68879.

[5] Kuzmanovic, A., & Knightly, E. W. (2003, August). Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (pp. 75-86).

[6] Liu, L., Wang, H., Wu, Z., & Yue, M. (2020). The detection method of low-rate DoS attack based on multi-feature fusion. Digital Communications and Networks, 6(4), 504-513.

[7] Maxwell, A. E., Warner, T. A., & Guillén, L. A. (2021). Accuracy assessment in convolutional neural network-based deep learning remote sensing studies—part 1: Literature review. Remote Sensing, 13(13), 2450.

[8] Tang, D., Dai, R., Tang, L., & Li, X. (2020). Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis. Human-centric Computing and Information Sciences, 10(1), 1-20.

[9] Tang, D., Tang, L., Dai, R., Chen, J., Li, X., & Rodrigues, J. J. (2020). MF-Adaboost: LDoS attack detection based on multi-features and improved Adaboost. Future Generation Computer Systems, 106, 347-359.

[10] Tang, D., Tang, L., Shi, W., Zhan, S., & Yang, Q. (2021). MF-CNN: a new approach for LDoS attack detection based on multi-feature fusion and CNN. Mobile Networks and Applications, 26(4), 1705-1722.

[11] Xie, R., Xu, M., Cao, J., & Li, Q. (2019, May). SoftGuard: Defend against the low-rate TCP attack in SDN. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[12] Yan, Y., Tang, D., Zhan, S., Dai, R., Chen, J., & Zhu, N. (2019, August). Low-rate dos attack detection based on improved logistic regression. In 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 468-476). IEEE.

[13] Yue, M., Wang, H., Liu, L., & Wu, Z. (2020). Detecting DoS attacks based on multi-features in SDN. IEEE Access, 8, 104688-104700.

[14] Zhan, S., Tang, D., Man, J., Dai, R., & Wang, X. (2019). Low-rate dos attacks detection based on maf-adm. Sensors, 20(1), 189.

[15] Zhang, D., Tang, D., Tang, L., Dai, R., Chen, J., & Zhu, N. (2019, August). Pca-svm-based approach of detecting low-rate dos attack. In 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1163-1170). IEEE.

[16] Zhang, T., Ramakrishnan, R., & Livny, M. (1996). BIRCH: an efficient data clustering method for very large databases. ACM sigmod record, 25(2), 103-114.

[17] Zhijun, W., Wenjing, L., Liang, L., & Meng, Y. (2020). Low-rate DoS attacks, detection, defense, and challenges: A survey. IEEE access, 8, 43920-43943.

18.2- المراجع الإلكترونية:

[18] http://mininet.org/ last visited at: 8.25.2021.

[19] https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.KFold.html last visited at 1.3.2022.

[20] https://scikit-learn.org/stable/modules/generated/sklearn.cluster.Birch.html last visited at 1.3.2022.

[21] https://scikit-learn.org/stable/modules/generated/sklearn.cluster.Birch.html last visited at 1.3.2022.

[22] https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LogisticRegression.html last visited at 1.3.2022

[23] https://scikit-learn.org/stable/modules/generated/sklearn.metrics.confusion_matrix.html last visited at 1.3.2022.

[24] https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.GridSearchCV.html last visited at 1.3.2022.

[25] https://scikit-learn.org/stable/modules/generated/sklearn.neighbors.KNeighborsClassifier.html last visited at 1.3.2022

[26] https://scikit-learn.org/stable/modules/generated/sklearn.neighbors.KNeighborsClassifier.html last visited at 1.3.2022.

[27] https://scikit-learn.org/stable/modules/generated/sklearn.neural_network.MLPClassifier.html last visited at 1.3.2022.

[28] https://scikit-learn.org/stable/modules/generated/sklearn.neural_network.MLPClassifier.html

last visited at 1.3.2022

[29] https://www.analyticsvidhya.com/blog/2020/07/what-is-skewness-statistics/
last visited at 1.3.2022.

[30] https://www.analyticsvidhya.com/blog/2021/05/shape-of-data-skewness-and-kurtosis/
last visited at 1.3.2022.

[31] https://www.ibm.com/cloud/learn/neural-networks
last visited at 1.3.2022.

[32] https://www.researchgate.net/figure/The-technique-of-KFold-cross-validation-illustrated-here-for-the-case-K-4-involves_fig10_278826818
last visited at 1.3.2022.

[33] https://zephyrnet.com/statistics-for-data-science-what-is-skewness-and-why-is-it-important/
last visited at 1.3.2022.