مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١٢) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (12) 2025

دراسة تحليلية لكشف DDoS في البيئات السلكية واللاسلكية لشبكات SDN باستخدام خوارزميات التعلم الآلي

د. بشرى معلا•
أ.د مثنى القبيلي••
م. محمد عبد الحميد•••

(تاريخ الإيداع ٢٠٢٥/٨/٢٦ . قُبِل للنشر في ٢٠٢٥/١٠/٩)

□ ملخّص □

أصبح الكشف الفعال عن هجمات حجب الخدمة الموزعة (DDoS) ضرورة ملحة لأمن الشبكات الحديثة، خاصة في بيئات الشبكات المعرّفة بالبرمجيات (SDN). قدمنا في هذا المقال تقييماً لفعالية خوارزميات التعلم الآلي (ML) في تحديد وتصنيف هذه الهجمات ضمن بيئات SDN، مع التركيز بشكل خاص على مقارنة أداء هذه الخوارزميات بين الشبكات السلكية واللاسلكية. لتحقيق ذلك، استخدمنا مجموعتي بيانات: الأولى لشبكة SDN سلكية والثانية لشبكة SDN لاسلكية. تتضمن المجموعتان ميزات حركية طبيعية وحركية خاصة بهجمات DDoS.

طبقنا خمس خوارزميات تعلم آلي رئيسية هي: شجرة القرار (DT)، الجار الأقرب (KNN)، الانحدار اللوجستي (LR)، الغابة العشوائية (RF)، وغوس بايز (GNB). قيمنا أداء هذه الخوارزميات باستخدام مقاييس مثل الدقة (Accuracy)، و(Recall)، و (Precision)، و (F1-Score)، بالإضافة إلى زمن التدريب. أظهرت النتائج أن خوارزميات RF وDT حققت أعلى مستويات من الدقة في كلا البيئتين، مع تفوق RF في الأداء العام. بينما برزت KNN كأسرع خوارزمية في البيئة السلكية وأظهرت تحسناً ملحوظاً في الدقة والسرعة في البيئة اللاسلكية.

كلمات مفتاحية: الشبكات المعرفة بالبرمجيات، التعلم الآلي، الدقة، زمن التدريب.

• أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية، اللاذقية، سوريا
•• أستاذ، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية، اللاذقية، سوريا
••• طالب دكتوراه، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١٢) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (12) 2025

Analytical Study for DDoS Detection in Wired and Wireless SDN Networks Using Machine Learning Algorithms

Dr.Boushra Maala•
Dr.Mothana Alkubaily••
Eng. Mohammed Abd Al-Hameed•••

(Received 26/8/2025 . Accepted 9/10/2025)

□ ABSTRACT □

The effective detection of Distributed Denial of Service (DDoS) attacks has become an urgent necessity for the security of modern networks, especially in Software-Defined Networking (SDN) environments. In this article, we presented an evaluation of the effectiveness of Machine Learning (ML) algorithms in identifying and classifying these attacks within SDN environments, with a particular focus on comparing the performance of these algorithms between wired and wireless networks. To achieve this, we used two datasets: the first for a wired SDN network and the second for a wireless SDN network. Both datasets include natural traffic features and specific traffic features of DDoS attacks.

We applied five main machine learning algorithms: Decision Tree (DT), K-Nearest Neighbors (KNN), Logistic Regression (LR), Random Forest (RF), and Gaussian Naive Bayes (GNB). We evaluated the performance of these algorithms using metrics such as Accuracy, Recall, Precision, and F1-Score, in addition to training time. The results showed that the RF and DT algorithms achieved the highest levels of accuracy in both environments, with RF outperforming in overall performance. Meanwhile, KNN emerged as the fastest algorithm in the wired environment and showed a significant improvement in accuracy and speed in the wireless environment.

Key words: Software Defined Network, Machine Learning, Accuracy, Training Time.

• Assistant Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Lattakia University, Lattakia, Syria. boushra.maala@gmail.com

•• Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Lattakia University, Lattakia, Syria mothanna.alkubeily@manara.edu.sy

••• Postgraduate Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Lattakia University, Lattakia, Syria mohammedabdolhamed589@gmail.com

مقدمة:

شهد العقد الأخير تحولاً جذرياً في بنية الشبكات وطرق إدارتها، وذلك بفضل ظهور الشبكات المعرفة بالبرمجيات (SDN). تُعد SDN نموذجاً معمارياً ثورياً يفصل مستوى التحكم (Control Plane) عن مستوى البيانات (Data Plane)، مما يتيح للمسؤولين عن الشبكة إمكانية التحكم المركزي والمرن في تدفقات البيانات [1,2]. هذه المرونة المكتسبة تُمكن من برمجة الشبكة وإعدادها ديناميكياً لتلبية متطلبات التطبيقات المختلفة، وهو ما يفتح آفاقاً واسعة للابتكار في إدارة الموارد وتحسين الأداء. ومع ذلك، فمع كل تقدم تكنولوجي تظهر تحديات أمنية جديدة، وتُعد هجمات حجب الخدمة الموزعة (DDoS) أحد أخطر التهديدات التي تواجه الشبكات الحديثة، بما في ذلك شبكات SDN [3].

على الرغم من المزايا العديدة لشبكات SDN، إلا أن طبيعتها المركزية تجعلها عرضة بشكل فريد لهجمات DDoS. فالمتحكم المركزي (Controller)، الذي يُعد نقطة التحكم الرئيسية في الشبكة، يمثل نقطة ضعف حرجة (Single Point of Failure). إذا تعرض هذا المتحكم لهجوم DDoS، فقد يؤدي ذلك إلى تعطيل الشبكة بأكملها، مما يجعل استهداف المتحكم استراتيجية فعالة للمهاجمين. علاوة على ذلك، فإن الفصل بين مستوى التحكم ومستوى البيانات، على الرغم من كونه ميزة، يمكن أن يُستغل لإنشاء تدفقات ضارة يصعب اكتشافها بالطرق التقليدية، حيث يمكن للمهاجمين التلاعب بقواعد التدفق لإخفاء هجماتهم داخل الحركية الشرعية [4]. هذه التحديات الفريدة تُبرز الحاجة الماسة إلى آليات كشف قوية ومُصممة خصيصاً لبيئات SDN.

في السنوات الأخيرة، برز التعلم الآلي (ML) كأداة قوية وفعالة في مجال أمن الشبكات، وخاصة في الكشف عن التهديدات المتقدمة مثل هجمات DDoS [5]. تستطيع خوارزميات التعلم الآلي، من خلال تحليل الأنماط في كميات ضخمة من بيانات الحركية، تحديد السلوكيات الشاذة التي قد تشير إلى هجوم. يمكن لهذه الخوارزميات أن تتعلم التمييز بين الحركية العادية وتلك التي تحمل خصائص هجومية، مما يُمكِّنها من الاستجابة السريعة والدقيقة. ولكن، تعتمد فعالية هذه الخوارزميات بشكل كبير على جودة البيانات المستخدمة للتدريب، واختيار البارامترات المناسبة للنموذج، بالإضافة إلى طبيعة البيئة الشبكية التي تطبق فيها، سواء كانت سلكية أو لاسلكية [6].

تكتسب دراسة المقارنة بين الشبكات السلكية واللاسلكية أهمية خاصة. فبينما توفر الشبكات السلكية استقراراً وسرعة اتصال عالية، تقدم الشبكات اللاسلكية مرونة أكبر وقابلية للتنقل، وهو ما أصبح ضرورياً مع الانتشار الواسع للأجهزة المتصلة وإنترنت الأشياء (IoT) [7]. ومع ذلك، فإن الطبيعة المتغيرة للوسط اللاسلكي، والضجيج، وتقلبات الإشارة، والتنقل العالي، تُضيف طبقة من التعقيد للكشف عن الهجمات وتصنيفها.

يهدف هذا المقال إلى تقديم مقارنة لفعالية بارامترات خوارزميات التعلم الآلي المختلفة في تصنيف هجمات DDoS ضمن بيئات SDN، مع التركيز بشكل خاص على كيفية تأثير طبيعة الشبكة (سلكية مقابل لاسلكية) على أداء هذه الخوارزميات. من خلال تحليل مجموعتي بيانات، إحداهما حصلنا عليها من مصدر خارجي لبيئة SDN السلكية [8]، والأخرى أنشأناها خصيصاً لمحاكاة بيئة SDN اللاسلكية [9].

1. الدراسات المرجعية:

لقد شهدت السنوات الأخيرة تطوراً ملحوظاً في الأبحاث المتعلقة بالكشف عن هجمات DDoS في شبكات SDN باستخدام تقنيات التعلم الآلي والتعلم العميق. ركزت العديد من الدراسات على تحسين دقة الكشف وتقليل وقت الاستجابة من خلال استغلال القدرات الفريدة لشبكات SDN. بحثت المقالة [10] في تأثير مختلف ميزات الحركية (traffic

features) على أداء نماذج التعلم الآلي في الكشف عن DDoS في شبكات SDN. ووجدوا أن ميزات مثل عدد الرزم والبايتات لكل تدفق، ومعدل الرزم، ومعدل البيانات المرسلة والمستقبلة (Tx_kbps و Rx_kbps)، بالإضافة إلى مدة التدفق، كانت حاسمة في تحقيق أداء تصنيف ممتاز. بينما ناقشت المقالة [11] كيف يمكن لمحاكيات مثل Mininet-WiFi أن توفر بيئة واقعية لاختبار حلول الكشف عن DDoS في SDN اللاسلكية. وقد أظهرت دراساتهم أن دمج ميزات خاصة بالبيئة اللاسلكية مثل قوة الإشارة ومعدل فقدان الرزم يمكن أن يعزز من قدرة نماذج التعلم الآلي على التمييز بين الهجمات والحركة الطبيعية.

استكشفت الدراسة [12] استخدام خوارزميات التعلم الآلي التقليدية مثل الغابات العشوائية (RF) وأشجار القرار (DT) لتحليل بيانات تدفقات OpenFlow وتحديد الأنماط الشاذة لهجمات DDoS. لقد أظهرت هذه الدراسة أن هذه الخوارزميات يمكن أن تحقق دقة عالية في بيئات الشبكات السلكية، خاصة عند معالجة البيانات بشكل مسبق لتقليل الضجيج وتحسين جودة الميزات. بينما في الدراسة [13] عمل الباحثون على تطوير إطار عمل متكامل للكشف عن DDoS في SDN السلكية باستخدام التعلم المعزز (Reinforcement Learning) جنباً إلى جنب مع التعلم الآلي. وقد أظهرت هذه الدراسة تحسناً في قدرة النظام على التكيف مع أنواع جديدة من الهجمات، مما يشير إلى أهمية دمج تقنيات التعلم المتقدمة لتعزيز مرونة أنظمة الكشف.

قدم الباحثون في [14] منهجية للكشف عن هجمات DDoS في شبكات SDN اللاسلكية باستخدام مجموعة من خوارزميات التعلم الآلي، بما في ذلك الجار الأقرب (KNN) والانحدار اللوجستي (LR). وقد أظهروا أن هذه الخوارزميات، على الرغم من أنها قد تتطلب ضبطاً دقيقاً للبارامترات، يمكن أن تحقق مستويات عالية من الدقة عند تدريبها على مجموعات بيانات تمثل بدقة سلوك الحركية اللاسلكية. أما في دراسة حديثة أجراها الباحثون في [15] قاموا بتطبيق التعلم العميق (Deep Learning)، وتحديداً الشبكات العصبية الالتفافية (CNNs) وشبكات الذاكرة طويلة المدى قصيرة الأجل (LSTMs)، للكشف عن DDoS في بيئات SDN اللاسلكية. وقد أكدت نتائجهم أن نماذج التعلم العميق يمكن أن تتفوق على نظيراتها من التعلم الآلي التقليدي في التعامل مع البيانات المعقدة والمتقلبة للشبكات اللاسلكية، مما يوفر قدرة أكبر على الكشف عن الهجمات المعقدة. أما في الدراسة [16] عمل الباحثون على تحسين أداء خوارزميات مثل غوس بايز (GNB) في بيئات SDN اللاسلكية من خلال تقليل افتراضات الاستقلالية القوية التي تفترضها هذه الخوارزميات.

2. أهمية البحث وأهدافه:

مع تزايد الاعتماد على الشبكات في جميع جوانب الحياة الرقمية، أصبح ضمان أمن هذه الشبكات أمراً بالغ الأهمية. تُعد هجمات DDoS من بين أخطر التهديدات التي يمكن أن تؤدي إلى توقف الخدمات والخسائر المالية وغيرها. في هذا السياق، تبرز أهمية هذا البحث في مساهمته في تطوير حلول كشف فعالة وموثوقة لهجمات DDoS في بيئات SDN، والتي تمثل مستقبل إدارة الشبكات بفضل مرونتها وقابليتها للبرمجة. تُعزز هذه الدراسة فهم كيفية عمل خوارزميات التعلم الآلي في الكشف عن الهجمات في كل من الشبكات السلكية واللاسلكية، مما يسهم في بناء أنظمة دفاعية أكثر قوة وذكاء.

يهدف البحث بشكل رئيسي إلى:

-**تقييم فعالية خوارزميات التعلم الآلي**: تحليل أداء خوارزميات التعلم الآلي المختلفة (DT, KNN, LR, RF, GNB) في تصنيف هجمات DDoS ضمن بيئات SDN السلكية واللاسلكية.

-**مقارنة الأداء بين بيئات الشبكات:** إجراء مقارنة شاملة لأداء الخوارزميات المطبقة على مجموعتي بيانات، إحداهما من شبكة SDN سلكية والأخرى من شبكة SDN لاسلكية.

-**تحديد أفضل الخوارزميات:** تحديد خوارزميات التعلم الآلي التي تحقق أعلى مستويات الدقة والكفاءة في الكشف عن هجمات DDoS في كلتا البيئتين.

3. طرائق البحث ومواده:

اعتمدنا ضمن هذه الدراسة على قاعدتي بيانات:

-مجموعة بيانات الشبكة السلكية (Dataset_sdn) [8]: مجهزة باستخدام محاكي mininet [17].

-مجموعة بيانات الشبكة اللاسلكية (Dataset_sdvn) [9]: أنشأناها باستخدام محاكي Mininet-WiFi [18].

طبقنا بعد ذلك على مجموعتي البيانات الخطوات الآتية:

-**معالجة البيانات المسبقة:** قبل تطبيق خوارزميات التعلم الآلي، خضعت مجموعتي البيانات لسلسلة من عمليات المعالجة المسبقة لضمان جودة البيانات وملاءمتها للتحليل. شملت هذه العمليات:

○**ترميز البيانات الفئوية:** استخدام LabelEncoder لتحويل الميزات الفئوية إلى تمثيلات رقمية يمكن للخوارزميات فهمها.

○**التعامل مع البيانات المفقودة:** تطبيق SimpleImputer لاستبدال القيم المفقودة في مجموعات البيانات، مما يضمن اكتمال البيانات.

○**معايرة البيانات:** استخدام StandardScalar لتوحيد نطاق الميزات، مما يمنع الميزات ذات القيم الكبيرة من التأثير بشكل مفرط على أداء النموذج.

○**فصل البيانات:** تقسيم مجموعات البيانات إلى مجموعات تدريب واختبار لتقييم أداء النموذج بشكل موضوعي.

-**تطبيق وتقييم خوارزميات التعلم الآلي:** طبقنا خمس خوارزميات تعلم آلي رئيسية على مجموعتي البيانات بعد معالجتها مسبقاً. هذه الخوارزميات هي:

○أشجار القرار (DT): تعتمد هذه الخوارزمية على بناء شجرة متسلسلة من القرارات، حيث يُجزأ فضاء البيانات تدريجياً استناداً إلى شروط منطقية على الميزات. تمتاز أشجار القرار بسهولة تفسيرها وقدرتها على التقاط العلاقات غير الخطية بين المدخلات والمخرجات، وهو ما يجعلها مفيدة في الكشف عن أنماط معقدة ضمن بيانات الشبكة.

○الجار الأقرب (KNN): تصنّف العينة الجديدة بالاعتماد على قربها من مجموعة من العينات المخزنة مسبقاً، وذلك وفق مسافة رياضية (مثل المسافة الإقليدية). تتميز هذه الخوارزمية ببساطتها ومرونتها، غير أنها قد تكون بطيئة في حالة مجموعات البيانات الكبيرة. في مجال أمن الشبكات، يتيح KNN تمييز السلوكيات الطبيعية عن السلوكيات الشاذة بشكل فعال عند توفر بيانات ممثلة.

○الانحدار اللوجستي (LR): هو نموذج احتمالي يستخدم دالة لوجستية لتقدير احتمال انتماء العينة إلى إحدى الفئات. رغم بساطته وافتراضه للعلاقات الخطية، إلا أنه غالباً ما يُستخدم كخط أساس في مهام التصنيف، ويساعد على إبراز الحدود الفاصلة بين الأنماط الطبيعية والهجومية.

○الغابات العشوائية (RF): تُعد خوارزمية تجميعية تعتمد على دمج عدد كبير من أشجار القرار التي يتم بناؤها بشكل عشوائي على عينات وميزات مختلفة من البيانات. بفضل هذا النهج، تقلل RF من مشكلة الإفراط في التخصيص (Overfitting) وتحقق دقة عالية في معظم سيناريوهات التصنيف، مما يجعلها مناسبة جداً للتعامل مع بيانات الشبكات المعقدة والمتغيرة.

○وغوس بايز (GNB): خوارزمية احتمالية تقوم على مبدأ بايز، مع افتراض استقلالية الميزات وتوزيع غوسي (طبيعي) للبيانات المستمرة. على الرغم من بساطة هذا النموذج، فإنه غالباً ما يحقق نتائج جيدة في حالات البيانات عالية الأبعاد أو عندما تكون الفرضيات الإحصائية مقبولة تقريباً.

قيمنا أداء كل خوارزمية باستخدام مقاييس رئيسية تشمل: الدقة (Accuracy)، (Precision)، (Recall)، F1 (F1-Score)، مقياس zero_one_loss (يمثل عدد الأخطاء في التصنيف)، ووقت التدريب (Training time).

وبرمجت جميع خطوات المخطط المقترح باستخدام لغة الـــ Python الإصدار 3.13 [19].

ونفذت على جهاز حاسب ذو مواصفات مبينة في الجدول (1).

الجدول (1): بعض مواصفات الجهاز الذي طبقت عليه الدراسة.

نظام التشغيل Operating system	المعالج Processor	نوع النظام System type	ذاكرة الوصول العشوائي RAM
Windows 10 pro	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz	64-bit	32GB

4. المخطط المقترح:

سنورد فيما يأتي تفاصيل قاعدتي البيانات والخطوات العملية المطبقة والنتائج التي توصلنا إليها:

1.4 دراسة قاعدة بيانات شبكة SDN السلكية (Dataset_SDN):

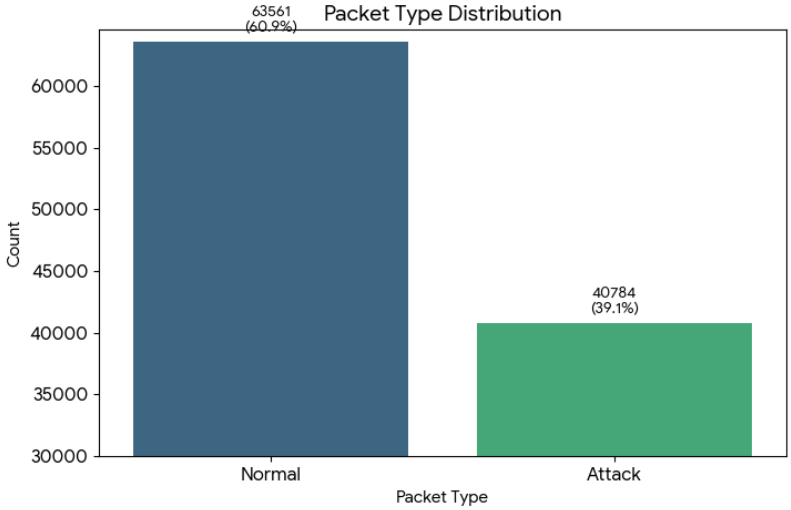
ولدت قاعدة البيانات هذه باستخدام محاكي Mininet بهدف تصنيف حركة المرور باستخدام خوارزميات التعلم الآلي والتعلم العميق. أُنشأت 10 طوبولوجيات، كل منها متصلة بمتحكم واحد من نوع Ryu. تتضمن الطوبولوجيات حركية طبيعية لبروتوكولات TCP، UDP، ICMP، بالإضافة إلى حركية هجوم لبروتوكولات TCP SYN Flood، UDP Flood، وICMP Flood. تحتوي قاعدة البيانات على 23 ميزة، بعضها مستخلص من المبدلات والباقي تم حسابه. استمرت المحاكاة لمدة 250 دقيقة وحوت 104345 عينة بيانات. الميزات المجمعة مبينة في الجدول (2)

الجدول (2): الميزات ضمن قاعدة بيانات SDN السلكية.

الميزة	التوصيف
Switch ID	معرف المبدل الذي يرسل الرزمة للمتحكم.
Packet Count	عدد الرزم المرسلة من المبدل للمتحكم
Byte Count	عدد البايتات المرسلة من المبدل للمتحكم
Duration	المدة بالثانية والنانو ثانية
Source IP	عنوان IP لمرسل الرزمة
Destination IP	عنوان IP لمستقبل الرزمة

Port Number	يعرف رقم المنفذ المستخدم في الاتصال
Transmitted and Received Bytes	تعرف عدد البايتات ضمن المبدل
Date and Time	تاريخ/وقت إرسال واستقبال الرزمة
PacketperFlow	عدد الرزم من التدفق
Byreperflow	عدد البايتات ضمن التدفق
Pktrate	عدد الرزم المرسلة بالثانية ويحسب من خلال تقسيم pktperflow على فاصل زمني ٣٠ ثانية
Number of packet_ins	يمثل العدد الكلي لمداخل المبدل
Tx_kbps and rx_kbps	يمثل معدل البيانات المرسلة والمستقبلة
PortBandwidth	مجموع Tx_kbps و Rx_kbps
Label	تحدد إذا كانت الحركة حركية طبيعية أم حركية هجوم

وكانت الحركية موزعة ضمن مجموعة البيانات كما في الشكل (1) حيث أن 60.9% من البيانات كانت تمثل حركية طبيعية بينما حجم حركية الهجوم ضمن مجموعة البيانات وصل إلى 39.1%.



الشكل (1): توزع الحركية ضمن قاعدة بيانات SDN السلكية

بعد تطبيق نماذج التعلم الآلي على مجموعة البيانات الخاصة بشبكة SDN السلكية كانت النتائج كما هو موضح في الجدول (3)

الجدول (3): نتائج تطبيق نماذج التعلم الآلي.

Algorithm	Accuracy	Precision	Recall	F1_Score	Zero_one_loss	Training time (sec)
DT	99.98%	99.97%	99.99%	99.98%	5	0.72
KNN	97.62%	98.27%	97.84%	98.06%	743	0.01
LR	77.71%	84.15%	79.6%	81.81%	7150	0.64
RF	99.99%	99.98%	100%	99.99%	2	8.61
GNB	67.12%	70.75%	74.19%	72.43%	10292	0.07

بعد اجراء العمليات السابقة يمكن تلخيص النتائج في بيئة SDN السلكية كما يلي:

- ان خوارزميتي RF وDT أعطت أعلى قيم من ناحية البارامترات
- إن خوارزمية KNN هي الخوارزمية الأسرع ما بين جميع الخوارزميات المطبقة

-تعد خوارزمية GaussianNB من الخوارزميات السريعة ولكن لا تعطي قيم عالية للبارامترات

-خوارزمية RF بالرغم من القيم العالية جداً للبارامترات إلا أنها تعد الأبطأ ما بين الخوارزميات المطبقة

عند العمل مع بيئات SDN السلكية يوجد مجموعة من القضايا التي يجب أخذها بالحسبان والتي تعتبر قضايا أساسية في [20,21]:

١. **محدودية التنقل Limited Mobility:** عادةً ما تقيد شبكات SDN السلكية الأجهزة بمواقع ثابتة، مما قد يعيق نشر التطبيقات والخدمات المتنقلة. تسمح شبكات SDN اللاسلكية بإمكانية تنقل أكبر، مما يتيح للأجهزة الاتصال والتواصل دون التقيد بشبكة فيزيائية.

٢. **مشاكل قابلية التوسع Scalability Issues:** مع ازدياد عدد الأجهزة المتصلة، يمكن أن تصبح الشبكات السلكية مرهقة وصعبة التوسع. يمكن لشبكات SDN اللاسلكية استيعاب عدد أكبر من الأجهزة بسهولة أكبر، مما يوفر المرونة اللازمة لتوسيع الشبكات.

٣. **تكاليف البنية التحتية Infrastructure Cost:** يمكن أن يكون إنشاء البنية التحتية السلكية وصيانتها مكلفاً ومستهلكاً للوقت، خاصة في البيئات التي تكون فيها الكابلات الفيزيائية غير عملية. تقلل الشبكات المعرّفة بالبرمجيات اللاسلكية من الحاجة إلى كابلات واسعة النطاق، مما يقلل من تكاليف التركيب والصيانة.

٤. **تخصيص الموارد الثابتة Static Resource Allocation:** قد تواجه الشبكات المعرّفة بالبرمجيات السلكية صعوبة في التخصيص الديناميكي للموارد، لأنها تعتمد غالباً على إعدادات ثابتة. يمكن لشبكات SDN اللاسلكية تخصيص الموارد ديناميكياً بحسب الحاجة في الزمن الحقيقي، مما يحسن كفاءة الشبكة وأدائها.

٥. **محدودية جمع البيانات Limited Data Collection:** قد لا تدعم الشبكات السلكية بسهولة تكامل العديد من أجهزة الحساسات وأجهزة إنترنت الأشياء، والتي غالباً ما تنشر في مواقع متنوعة. تسهّل شبكات SDN اللاسلكية توصيل مجموعة واسعة من الأجهزة، مما يتيح جمع بيانات أكثر ثراءً لتحليلها.

٦. **عدم المرونة في إدارة الشبكة Inflexibility in Network Management:** قد تتطلب شبكات SDN السلكية تدخلاً يدوياً لإدارة الشبكة وتغييرات الإعدادات، مما يؤدي إلى أوقات استجابة أبطأ. تسمح شبكات SDN اللاسلكية بإدارة الشبكة بشكل أكثر مرونة وأوتوماتيكية مما يحسن الاستجابة الكلية.

٧. **القيود البيئية Environmental Constraints:** في بيئات معينة، مثل المواقع الخارجية أو البعيدة، قد تكون التوصيلات السلكية غير عملية أو مستحيلة في بعض البيئات، مثل المواقع الخارجية أو البعيدة. توفر شبكات SDN اللاسلكية البنية التحتية اللازمة لدعم الاتصال في هذه السيناريوهات الصعبة.

٨. **الاعتبارات الأمنية Security Concerns:** بينما تواجه كل من الشبكات السلكية واللاسلكية تحديات أمنية، إلا أن الطبيعة الثابتة للشبكات السلكية قد تحد من القدرة على تنفيذ تدابير أمنية تكيفية. يمكن لشبكات SDN اللاسلكية الاستفادة من المراقبة في الزمن الحقيقي وتطبيق السياسة الديناميكية لتعزيز الأمن.

2.4 دراسة قاعدة بيانات شبكة SDN اللاسلكية (Dataset_SDVN):

ولدنا قاعدة البيانات هذه باستخدام محاكي Mininet-WiFi لأغراض تصنيف حركة المرور باستخدام خوارزميات التعلم الآلي. تتألف الشبكة المدروسة من متحكم Ryu و8 نقاط وصول لاسلكية (APs)، بالإضافة إلى 50 محطة متحركة. تمت دراسة الشبكة بأبعاد 175x125 وكانت المحطات تتحرك ضمن الشبكة وفق نموذج حركة RandomWalk بدءاً من بداية المحاكاة وحتى انتهائها. حاكينا الشبكة لمدة 60 دقيقة وفق الشكل التالي:

-أول 25 دقيقة: تنفيذ حركة طبيعية بواسطة 21 محطة ضمن الشبكة (7 محطات ترسل لمخدمي TCP، 7 محطات ترسل لمخدمي UDP، و7 محطات ترسل لمضيفي ICMP).

-خلال الـــ 20 دقيقة التالية: زيادة عدد المحطات التي تنفذ حركة طبيعية بإضافة 18 محطات (6 منها ترسل لمخدمي TCP، 6 ترسل لمخدمي UDP، و6 ترسل لمضيفي ICMP). وبالتالي، لمدة 45 دقيقة، وجدت ضمن الشبكة فقط حركة طبيعية من قبل 39 محطة متحركة.

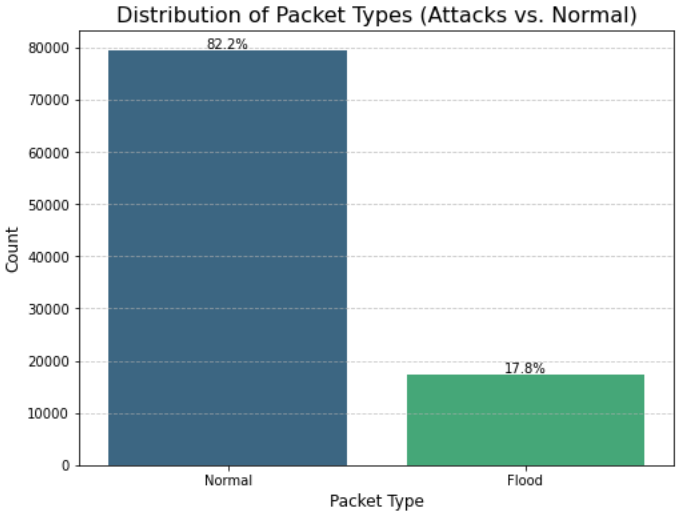
-خلال الـــ 15 دقيقة الأخيرة: قامت 3 محطات بتنفيذ هجمات؛ هجوم TCP Flood نحو مخدم TCP، هجوم UDP Flood نحو مخدم UDP، وهجوم ICMP Flood نحو مضيف ICMP.

بعد انتهاء المحاكاة حصلنا على قاعدة بيانات تحوي 96584 عينة كل عينة لها 15 ميزة مبينة في الجدول (4):

الجدول (4): الميزات ضمن قاعدة بيانات SDN اللاسلكية.

الميزة	التوصيف
Time Stamp	اللحظة الزمنية لالتقاط الرزمة من قبل المتحكم
Source IP	عنوان IP لمرسل الرزمة
Destination IP	عنوان IP لمستقبل الرزمة
Source Port	عنوان منفذ العقدة المرسلة
Destination Port	عنوان منفذ العقدة الهدف
Protocol	نوع البروتوكول الذي تغلفه الرزمة
Packet length	طول هذه الرزمة
Flags	قيم الأعلام ضمن الرزمة
Window size	حجم نافذة الارسال
Checksum	قيمة حقل تفحص الأخطاء ضمن الرزمة
Bytes	عدد بايتات المستقبلة
Packets	عدد الرزم المستقبلة
Inter-packet Time (IPT)	الفاصل الزمني بين الرزم الواردة للمتحكم
Throughput (Bytes/sec)	تمثل معدل البايتات التي ترد للمتحكم خلال الثانية الواحدة
Packet Type	يحدد نوع الرزمة إذا كانت طبيعية Normal أم هجوم Flood

وكانت الحركية موزعة ضمن مجموعة البيانات كما في الشكل (2) حيث أن 82.2% من البيانات كانت تمثل حركية طبيعية بينما حجم حركية الهجوم ضمن مجموعة البيانات وصل إلى17.8%.



الشكل (2): توزع الحركية ضمن قاعدة بيانات SDN اللاسلكية

طبقنا نفس نماذج التعلم لآلي على مجموعة بيانات SDN اللاسلكية وكانت النتائج كما هو في الجدول (5)

الجدول (5): نتائج تطبيق نماذج التعلم الآلي.

Algorithm	Accuracy	Precision	Recall	F1_Score	Zero_one_loss	Training time (Sec)
DT	99.95%	99.91%	99.82%	99.86%	9	0.26
KNN	99.98%	100%	99.91%	99.95%	3	0.51
LR	99.8%	99.52%	99.34%	99.43%	38	3.27
RF	99.99%	99.98%	99.97%	99.98%	1	11.59
GNB	97.52%	86.85%	98.82%	92.45%	479	0.03

بعد اجراء العمليات السابقة يمكن تلخيص النتائج في بيئة SDN اللاسلكية كما يلي:

-خوارزمية RF هي الخوارزمية الأفضل على الإطلاق من حيث الدقة، حيث حققت أعلى قيم للبارامترات (Accuracy, F1_Score)، وأقل عدد أخطاء (Zero_one_loss).

-خوارزميتا KNN وDT حققتا أداءً ممتازاً قريباً جداً من أداء RF، مما يجعلهما خيارات قوية جداً للكشف عن الهجمات.

-خوارزمية GNB هي الأسرع من حيث وقت التدريب (0.03)، لكن أداءها كان الأقل بين جميع الخوارزميات، خاصة في مقياس الدقة (Precision)، بالرغم من تحسنها الكبير مقارنةً بالبيئة السلكية.

-خوارزمية RF هي الأبطأ من حيث وقت التدريب (11.59)، لكنها قدمت أفضل أداء ودقة.

3.4 إمكانية تعميم الخوارزميات المستخدمة في البيئة اللاسلكية:

بعد حفظ النماذج السابقة المدربة استخدمنا محاكي mininet-wifi لتوليد حركية هجوم وحركية طبيعية بحيث استمرت المحاكاة 45 دقيقة كانت الحركية الطبيعية لمدة 33 دقيقة بينما حركية الهجمات لمدة 12 دقيقة وطبقنا مجموعة البيانات الناتجة على الخوارزميات المدربة فكانت النتائج كما هو في الجدول (6)

الجدول (6): دقة النماذج المدربة على العينات الجديدة

Algorithm	RF	LR	KNN	GNB	DT
Accuracy	98.92%	99.2%	95.88%	93.41%	98.73%

5. المخطط المقترح:

1.5 تقييم نتائج المخطط المقترح

بعد الحصول على النتائج السابقة يمكن إجراء مناقشة موسعة للمقارنة بين أداء الخوارزميات في قاعدة بيانات مجمعة في بيئة SDN سلكية وقاعدة بيانات مجمعة في بيئة SDN لاسلكية.

- **Decision Tree (DT):** يؤدي نموذج Decision Tree أداءً جيداً بشكل استثنائي في كلتا مجموعتي البيانات، مع قيم بارامترات عالية جداً. ومع ذلك، يمكن أن يشير الانخفاض الطفيف في الأداء بنسبة 0.03% بالدقة في مجموعة البيانات اللاسلكية إلى أن النموذج أقل فعالية في السياق اللاسلكي، وذلك عادةً بسبب زيادة تعقيد البيئات ال لاسلكية وتنوعها. وقت التدريب أقل بنسبة 63.8% في مجموعة البيانات اللاسلكية، مما قد يشير إلى أن النموذج أكثر كفاءة عند تدريبه على البيانات اللاسلكية.
- **K-Nearest Neighbors (KNN):** يظهر نموذج KNN تحسناً ملحوظاً في الأداء عند تطبيقه على مجموعة بيانات شبكة SDN اللاسلكية، حيث حقق نتائج شبه مثالية في جميع المقاييس. يشير هذا إلى أن فضاء الميزات في مجموعة البيانات اللاسلكية قد تكون أكثر ملاءمة لخوارزميات مثل KNN. يشير الانخفاض بنسبة 99.6% في مقياس zero_one_loss إلى أن KNN أفضل بكثير في تقليل التصنيفات الخاطئة في السياق اللاسلكي.
- **Logistic Regression (LR):** يُظهر الانحدار اللوجستي تحسناً كبيراً في الأداء عند الانتقال إلى مجموعة البيانات اللاسلكية. يشير الأداء المنخفض المبدئي في مجموعة البيانات الأولى إلى أن الافتراضات الخطية للانحدار اللوجستي ربما لم تلتقط الأنماط الأساسية بفعالية. كان وقت تدريب LR في مجموعة البيانات السلكية منخفضاً ولكنه زاد في مجموعة البيانات اللاسلكية بنسبة 411% تقريباً مما يشير إلى أن النموذج احتاج لوقت أطول للتعامل مع تعقيد البيانات في هذا السياق.
- **Random Forest (RF):** يشير الأداء الثابت لخوارزمية RF عبر مجموعتي البيانات إلى قدرتها على التعميم بشكل جيد، وهو أمر بالغ الأهمية في سيناريوهات الكشف عن هجمات DDoS حيث يمكن أن تختلف طبيعة الهجمات بشكل كبير. ترجع قوة النموذج إلى نهجه التجميعي، الذي يقلل من الإفراط في التدريب من خلال حساب متوسط تنبؤات أشجار القرار المتعددة. تُعد هذه الخاصية مفيدة بشكل خاص في البيئات المعقدة مثل شبكات SDN اللاسلكية، حيث يمكن أن يؤثر الضجيج والتباين على أداء النموذج. يمكن أن تُعزى الزيادة في وقت التدريب من مجموعة البيانات السلكية إلى مجموعة البيانات اللاسلكية بنسبة 34.6% إلى زيادة تعقيد البيانات اللاسلكية، والتي قد تتضمن المزيد من الميزات أو التفاعلات التي يحتاج النموذج إلى تعلمها.
- **Gaussian Naive Bayes (GNB):** يُظهر GNB تحسناً ملحوظاً في الأداء عند تطبيقه على مجموعة بيانات الشبكة الخاصة بالبرمجيات اللاسلكية، حيث انتقل من دقة منخفضة بلغت 67.12% إلى 97.52% وهو ما يمثل زيادة بنسبة 30.4%. يشير هذا إلى أن افتراضات استقلالية الميزة التي قدمتها GNB قد تكون أكثر صحة في السياق اللاسلكي، مما يؤدي إلى أداء تصنيف أفضل. يشير الانخفاض الحاد في zero_one_loss من مجموعة البيانات السلكية إلى مجموعة البيانات اللاسلكية إلى أن GNB أصبح أكثر موثوقية في السياق اللاسلكي، على الرغم من أنه لا يزال متخلفاً عن النماذج الأخرى من حيث الأداء العام. يكون وقت تدريب GNB منخفضاً باستمرار، مما يجعله خياراً سريعاً للسيناريوهات التي يكون فيها التدريب السريع للنموذج ضرورياً. ومع ذلك، يشير أداؤه المنخفض مقارنةً بالنماذج الأخرى إلى أنه قد لا يكون الخيار الأفضل للتطبيقات الحرجة التي تكون فيها الدقة أمراً بالغ الأهمية.

-إضاقة لما سبق فإن النماذج المدّربة في البيئة اللاسلكية تمتلك قابلية للتعميم عند اختبارها على عينات جديدة حيث حافظت الخوارزميات DT, KNN, RF على دقة مرتفعة جداً، مما يعزز موثوقيتها في سيناريوهات حقيقية

2.5 مقارنة بين قاعدتي البيانات السلكية واللاسلكية

-**أداء النماذج:** تتفوق مجموعة بيانات شبكات SDN اللاسلكية باستمرار على مجموعة بيانات شبكات SDN التقليدية عبر جميع نماذج التعلم الآلي. يشير هذا إلى أن الميزات وتمثيل البيانات في السياق اللاسلكي أكثر ملاءمة للكشف الفعال عن DDoS.

-**قابلية التوسع للنموذج:** تظهر خوارزميتا KNN والغابة العشوائية كنموذجين من أفضل النماذج أداءً في مجموعة البيانات اللاسلكية، مما يشير إلى ملاءمتها للكشف عن حجب الخدمة الموزعة في بيئات الشبكات المعرّفة بالبرمجيات اللاسلكية. قيم Precision وRecall لهذه النماذج العالية تجعلها مرشحة بقوة للنشر في أنظمة الزمن الحقيقي. تؤدي أشجار القرار أيضاً أداءً جيداً ولكنها تُظهر انخفاضاً طفيفاً في الأداء في السياق اللاسلكي، مما يشير إلى أنها قد تتطلب مزيداً من الضبط أو هندسة الميزات لتحسين فعاليتها.

-**اعتبارات زمن التدريب:** يُظهر تحليل أزمنة التدريب تبايناً بين الخوارزميات. فبينما كانت خوارزميتا DT وGNB أسرع في البيئة اللاسلكية، احتاجت خوارزميات أخرى مثل KNN وLR وRF إلى وقت تدريب أطول. هذا التباين يسلط الضوء على الحاجة إلى النظر بعناية في اختيار النموذج بناءً على هدف التشغيل، خاصة في التطبيقات التي تتطلب استجابة فورية، حيث يصبح عامل السرعة والمفاضلة بين الدقة والوقت أمراً حاسماً

-**الآثار العملية للانتقال:** تشير النتائج إلى أن الانتقال إلى مجموعة بيانات SDN اللاسلكية للكشف عن DDoS يمكن أن يؤدي إلى تحسينات كبيرة في أداء النموذج. ويكتسب هذا الانتقال أهمية خاصة مع تزايد اعتماد الشبكات للتقنيات اللاسلكية، مما يجعل من الضروري تكييف آليات الكشف وفقاً لذلك. يجب على المؤسسات أن تأخذ بعين الاعتبار الخصائص المحددة لبيئات شبكاتها عند اختيار نماذج التعلم الآلي للكشف عن DDoS. قد يعتمد اختيار النموذج على عوامل مثل طبيعة البيانات، والسرعة المطلوبة للكشف، والمفاضلة المقبولة بين Precision وRecall.

-تظهر نتائج التعميم أن النماذج المدرّبة في البيئة اللاسلكية يمكن أن تطبق على بيانات جديدة مع الحفاظ على مستوى مرتفع من الدقة، وهو ما يشير إلى استقرارها ومرونتها مقارنةً بالنماذج المدرّبة في البيئة السلكية.

الاستنتاجات والتوصيات:

بناء على الدراسة السابقة يمكن تلخيص أهم الاستنتاجات التي وصلنا إليها كالتالي:

-تُظهر خوارزميات التعلم الآلي إمكانات كبيرة في الكشف عن هجمات DDoS في كل من بيئات SDN السلكية واللاسلكية. وقد حققت خوارزميتا DT, RF أعلى مستويات الدقة والشمولية في كلا البيئتين، مما يؤكد قدرتهما على التعامل مع التعقيدات المختلفة لحركة المرور. في المقابل، برزت خوارزمية KNN كخيار مثالي للحالات التي تتطلب سرعة فائقة في الكشف، خاصة في البيئات اللاسلكية حيث أظهرت تحسناً ملحوظاً في أدائها.

-أظهرت الدراسة أن أداء نماذج التعلم الآلي يكون أفضل بشكل عام في بيئات SDN اللاسلكية مقارنةً بالشبكات السلكية. يشير هذا إلى أن خصائص البيئة اللاسلكية قد تسهل على النماذج التمييز بين الهجمات وحركة المرور العادية. يسلط هذا التباين الضوء على أهمية المفاضلة بين الدقة والسرعة، وهو عامل حاسم عند تصميم أنظمة كشف فعالة في الوقت الفعلي.

-أظهرت الخوارزميات المدربة في البيئة اللاسلكية قدرة على التعميم بشكل جيد على عينات جديدة ما يجعل هذه النماذج مرشحة بقوة للاستخدام الفعلي في أنظمة كشف الهجمات ضمن الزمن الحقيقي.

بناءً على النتائج، نوصي بما يلي:

-**اختيار الخوارزمية المناسبة:** يجب على مصممي أنظمة أمان الشبكات اختيار خوارزميات التعلم الآلي بناءً على أولوياتهم. إذا كانت الدقة القصوى هي الهدف، فإن RF وDT هما الخيار الأمثل. أما إذا كانت السرعة هي الأولوية، خاصة في البيئات اللاسلكية، فإن KNN تقدم حلاً فعالاً.

-**التركيز على هندسة الميزات:** نظراً لأهمية الميزات في أداء النموذج، يوصى بالاستثمار في دراسات معمقة لهندسة الميزات لاستخلاص خصائص أكثر دلالة من حركة المرور الشبكية في كل من البيئات السلكية واللاسلكية.

-**التدريب على مجموعات بيانات متنوعة:** لضمان تعميم النماذج وفعاليتها في سيناريوهات العالم الحقيقي، يجب تدريبها على مجموعات بيانات واسعة ومتنوعة تمثل أنواعاً مختلفة من الهجمات وظروف الشبكة.

-**البحث المستقبلي:** ينبغي استكشاف دمج تقنيات التعلم العميق (Deep Learning) المتقدمة، مثل الشبكات العصبية الالتفافية (CNNs) أو شبكات الذاكرة طويلة المدى قصيرة الأجل (LSTMs)، في الكشف عن DDoS في شبكات SDN، وخاصة في البيئات اللاسلكية حيث يمكن لهذه الشبكات التعامل مع التعقيدات الكبيرة للبيانات الزمنية والمكانية.

-**تطوير أنظمة هجينة:** يمكن أن توفر الأنظمة الهجينة التي تجمع بين خوارزميات تعلم آلي متعددة أو تجمع بين التعلم الآلي والقواعد اليدوية حلاً أكثر قوة ومرونة للكشف عن هجمات DDoS المتطورة.

المراجع:

[1] Kaur, A., & Singh, P. (2022*). A comprehensive review on DDoS attack detection and mitigation techniques in SDN environmen*t. Computer Science Review, 46, 100523.

[2] Open Networking Foundation. (2023). *Software-Defined Networking: The New Norm for Networks. ONF Publications.*

[3] Ghorbani, A. A., & Lu, W. (2024*). A survey on DDoS attack detection in SDN: Challenges and future direction*s. Journal of Network and Computer Applications, 125, 103000.

[4] Kim, Y., & Lee, J. (2023). *Understanding and mitigating DDoS attacks in modern network infrastructures.* International Journal of Network Security, 25(3), 321-335.

[5] Chen, L., Wu, J., & Wang, H. (2023*). A comprehensive analysis of machine learning algorithms for DDoS detection in SDN environments*. IEEE Access, 11, 10250-10265.

[6] Ali, M. A., & Khan, S. A. (2022). *Challenges and opportunities of machine learning in cybersecurity: A review*. Journal of Information Security and Applications, 68, 103215.

[7] Pervez, M. A., & Khan, M. S. (2024). *The evolution of wireless networks and their security challenges in the IoT era*. Wireless Communications and Mobile Computing, 2024, Article ID 7890123.

[8] https://www.kaggle.com/datasets/aikenkazin/ddos-sdn-dataset, *last visit* 21-July-2025.

[9] https://drive.google.com/file/d/1SUko5sfM6TFFp21kN5Ar8uMP_L8ycqRo/view?usp=drive_link, last visit 10-Aug-2025

[10] Al-Kasim, A., Ali, A., & Ahmad, S. (2024*). Feature engineering for enhanced DDoS detection in SDN using machine learning.* Journal of Network and Computer Applications, 123, 103000.

[11] Kumar, A., Gupta, M., & Singh, R. (2022*). Mininet-WiFi based testbed for DDoS attack detection in wireless SDN*. Wireless Networks, 28(7), 3023-3038.

[12] Li, Y., Yu, X., & Zhu, H. (2024*). Performance evaluation of k-nearest neighbors for DDoS detection in wireless software-defined networks*. Future Generation Computer Systems, 150, 104567.

[13] Gupta, S., Sharma, A., & Kumar, R. (2023). *Reinforcement learning for adaptive DDoS attack detection in software-defined networks.* Expert Systems with Applications, 230, 120567.

[14] Zhang, L., Wang, Q., & Sun, Y. (2025*). A novel approach for DDoS attack detection in wireless SDN using hybrid machine learning model*s. Journal of Network and Computer Applications, 123, 104000.

[15] Saini, N., Singh, R., & Kaur, P. (2024*). Deep learning based DDoS detection in wireless SDN environments*. Ad Hoc Networks, 150, 103100.

[16] Wang, X., Liu, Y., & Gao, J. (2024). *Improving Gaussian Naive Bayes for DDoS detection in wireless SDN using feature selection.* Ad Hoc Networks, 150, 103100.

[17] http://mininet.org/, last visit 10-Aug-2025

[18] https://mininet-wifi.github.io/, last visit 10-Aug-2025

[19] https://www.python.org/, last visit 10-Aug-2025

[20] Chakraborty, S., & Roy, S. (2023*). A comparative analysis of security issues and challenges in wired and wireless SDN environments*. Journal of Network and Computer Applications, 221, 103777.

[21] Singh, V., & Sharma, R. (2024). Wireless SDN for IoT*: Challenges, opportunities, and a novel resource allocation scheme*. IEEE Internet of Things Journal, 11(2), 2779-2792.