مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (١٠) العدد (٧) ٢٠٢٦

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (7) 2026

كشف هجمات حجب الخدمة الموزعة (DDoS) في شبكات العربات المعرفة بالبرمجيات (SDVN) باستخدام تحليل تدفقي ونماذج التعلّم الآلي

د. بشرى معلا•

أ.د مثنى القبيلي••

م. محمد عبد الحميد•••

(تاريخ الإيداع ٢٠٢٦/٢/٥ . قُبِل للنشر في ٢٠٢٦/٤/٢٣)

□ ملخّص □

تُعدّ شبكات العربات المعرفة بالبرمجيات (SDVN) من البيئات الشبكية الديناميكية التي تعتمد على متحكم مركزي لإدارة الحركية، مما يجعلها عرضة لهجمات حجب الخدمة الموزعة (DDoS) ذات التأثير العالي على استقرار الشبكة. تهدف هذه الدراسة إلى تحليل سلوك الحركية والكشف عن هجمات DDoS في بيئة SDVN اعتماداً على مؤشرات تدفقية مستخرجة من محاكاة واقعية باستخدام Mininet–WiFi ومتحكم SDN من نوع Ryu. ولدت حركية طبيعية وخمسة أنماط رئيسية من الهجمات، وخضعت البيانات لمرحلة تنظيف وفحص جودة شاملة، وتحديد الميزات التي تملك التأثير الأكبر في تحديد نوع الحركية سواء طبيعية أم حركية هجوم.

بناءً على ذلك اعتمد البحث على مجموعة ميزات أساسية لتقييم أداء خوارزميات التعلّم الآلي التقليدية في مهمة تصنيف متعددة الفئات تشمل الحركة الطبيعية وخمسة أنماط من هجمات DDoS. شملت الخوارزميات المستخدمة أشجار القرار، الغابات العشوائية، الجار الأقرب، الانحدار اللوجستي، وغوس بايز وآلة دعم المتجه. أظهرت النتائج تفوق النماذج الشجرية، ولا سيما خوارزمية الغابة العشوائية، من حيث الدقة والاستقرار العام، مع ظهور أنماط التباس منطقية بين بعض الهجمات المتقاربة سلوكياً، مما يعكس واقعية التحدي في بيئات SDVN الديناميكية.

كلمات مفتاحية: شبكات العربات المعرفة بالبرمجيات، التعلم الآلي، حجب الخدمة الموسع، الدقة.

• أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية، اللاذقية، سوريا
boushra.maala@latakia-univ.edu.sy

•• أستاذ، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية، اللاذقية، سوريا
mothanna.alkubeily@latakia-univ.edu.sy

••• طالب دكتوراه، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
mohammed.abdulhamid@latakia-univ.edu.sy

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (١٠) العدد (٧) ٢٠٢٦

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (7) 2026

Detection of Distributed Denial-of-Service (DDoS) Attacks in Software-Defined Vehicular Networks (SDVN) Using Flow-Based Analysis and Machine Learning Models

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

(Received 5/2/2026 . Accepted 23/4/2026)

□ ABSTRACT □

Software-Defined Vehicular Networks (SDVNs) are considered dynamic networking environments that rely on a centralized controller to manage traffic, which makes them vulnerable to Distributed Denial of Service (DDoS) attacks with a high impact on network stability. This study aims to analyze traffic behavior and detect DDoS attacks in an SDVN environment based on flow indicators extracted from a realistic simulation using Mininet-WiFi and an SDN controller of type Ryu. Normal traffic and five main attack patterns were generated, and the data underwent a comprehensive cleaning and data-quality inspection stage, along with identifying the features that have the greatest impact in determining the type of traffic, whether normal traffic or attack traffic.

Based on this, the study relied on a set of core features was selected to evaluate the performance of traditional machine learning algorithms in a multi-class classification task that includes normal traffic and five patterns of DDoS attacks. The algorithms used include Decision Tree, Random Forest, K-Nearest Neighbors, Logistic Regression, Gaussian Naive Bayes, and Support Vector Machine. The results showed the superiority of tree-based models, particularly the Random Forest algorithm, in terms of accuracy and overall stability, with logical confusion patterns appearing between some attacks that are behaviorally similar, which reflects the realistic challenge in dynamic SDVN environments.

Keywords: Software-Defined Vehicular Networks, Machine Learning, Distributed Denial of Service, Accuracy.

• Assistant Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Latakia University, Latakia, Syria. Boushra.maala@latakia-univ.edu.sy

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

••• Postgraduate Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Lattakia University, Lattakia, Syria mohammed.abdulhamid@latakia-univ.edu.sy

مقدمة:

شهدت الشبكات المعرفة بالبرمجيات (Software–Defined Networking – SDN) اهتماماً متزايداً بوصفها بنية مرنة وقابلة للبرمجة تفصل مستوى التحكم عن مستوى تمرير البيانات، مما يحسن إدارة الحركية في الشبكات الديناميكية الحديثة (Batool et al., 2025). وقد امتد تطبيق هذا المفهوم إلى بيئات أكثر تعقيداً مثل شبكات العربات وإنترنت الأشياء التي تتطلب آليات تحكم قادرة على التكيف مع التغيرات السريعة في الحركية والتحميل الشبكي.

وفي هذا السياق ظهرت شبكات العربات المعرفة بالبرمجيات (SDVN) التي تستفيد من التحكم المركزي وقابلية البرمجة لتحسين إدارة الحركية واستغلال الموارد ودعم تطبيقات النقل الذكي منخفضة الكمون وعالية الموثوقية (Aslam et al., 2025). إلا أن الطبيعة الديناميكية لهذه البيئات والاعتماد على مكونات برمجية مركزية يزيدان من التحديات الأمنية مقارنة بالشبكات التقليدية.

تُعد هجمات DDoS من أبرز هذه التهديدات، إذ تستهدف إغراق المتحكم أو عناصر البنية التحتية بحركية كثيفة تؤدي إلى استنزاف الموارد وتعطيل عمليات التحكم واتخاذ القرار (Hill et al., 2024). وتزداد صعوبة كشف هذه الهجمات في البيئات الديناميكية مثل SDN وSDVN بسبب التغير المستمر في أنماط الحركية الشبكية.

وقد أظهرت الدراسات الحديثة محدودية الأساليب المعتمدة على القواعد أو العتبات الثابتة في كشف هجمات DDoS، بينما برزت تقنيات التعلّم الآلي (ML) كنهج فعّال لتحليل بيانات الحركية واستخلاص الأنماط السلوكية للتدفقات الشبكية اعتماداً على مؤشرات تدفقية وإحصائية. وتشير الأبحاث إلى أن دمج التحليل التدفقي مع خوارزميات التعلم الآلي يحقق نتائج واعدة في كشف هذه الهجمات في البيئات القريبة من SDVN (Babbar et al., 2024).

يهدف هذا المقال إلى تحليل سلوك الحركية في بيئة SDVN لاسلكية ودراسة تأثير هجمات DDoS على خصائص التدفقات الشبكية اعتماداً على بيانات مولدة من محاكاة واقعية، إضافة إلى تقييم أداء خوارزميات التعلّم الآلي التقليدية في مهمة تصنيف متعددة الفئات بعد تنفيذ مراحل تنظيف البيانات واختيار الميزات الأساسية، بهدف بناء خط أساس علمي يمكن الاعتماد عليه في تطوير نماذج كشف أكثر تقدماً.

1. الدراسات المرجعية:

شهد مجال كشف هجمات حجب الخدمة الموزعة (DDoS) في البيئات المعرفة بالبرمجيات تطوراً ملحوظاً خلال السنوات الأخيرة، حيث ركّزت العديد من الدراسات على توظيف خوارزميات التعلّم الآلي لتحسين دقة الكشف وتقليل العبء على متحكمات الشبكة. في هذا السياق، قدّم (Nadeem et al., 2022) إطاراً لكشف الهجمات في شبكات SDN التقليدية باستخدام مجموعة من الخوارزميات الكلاسيكية مثل RF وKNN وSVM، مع الاعتماد على مجموعة محدودة من الميزات الإحصائية. ورغم تحقيقه دقة تقارب 97%، إلا أن هذا العمل اقتصر على بيئة ثابتة دون حركية، ولم يتناول سيناريوهات شبكات العربات أو التأثيرات الديناميكية للحركة.

من ناحية اختيار الميزات، استخدمت دراسة (Hakeem and Attiah, 2024) أسلوب SelectKBest لاختيار الميزات الأكثر أهمية قبل تطبيق نماذج تعلم آلي متعددة. ورغم تحقيقها دقة تجاوزت 99%، إلا أن

التجارب أُجريت على مجموعات بيانات عامة ذات حركة غير واقعية، دون محاكاة للحركية أو خصائص شبكات العربات، مما يحد من قابلية تعميم النتائج على بيئات SDVN الحقيقية.

في المقابل، اتجهت بعض الأعمال إلى استخدام نماذج تعلّم عميق، مثل الدراسة (Elubeyd and Yiltas Kaplan, 2023)، التي حققت دقة مرتفعة جداً تجاوزت 99.8% في كشف هجمات DDoS ضمن بيئة SDN. ومع ذلك، تعاني هذه النماذج من تعقيد حسابي مرتفع، مما يجعلها أقل ملاءمة للتطبيقات الزمن الحقيقي، خاصة في البيئات الديناميكية مثل شبكات العربات.

على مستوى SDVN بشكل مباشر، قدّم الباحثون في (Babbar et al., 2024) إطاراً للكشف عن هجمات DDoS باستخدام تحليل إحصائي للتدفقات مع خوارزميات تعلم آلي تقليدية. ورغم تحقيق نتائج جيدة من حيث الدقة وF1–score، إلا أن الدراسة لم تعتمد حركية مستمرة للعربات، كما غابت فيها آليات العتبات الديناميكية، مما يقلل من واقعية السيناريو التجريبي.

مؤخراً، وسّعت الدراستين (Sarvade et al., 2025; Ababsa et al., 2025) نطاق البحث ليشمل شبكات العربات وإنترنت العربات (IoV)، مع استخدام نماذج متقدمة مثل الشبكات العصبية الهجينة والنماذج العميقة مع آليات الانتباه. ورغم الأداء المرتفع الذي حققته هذه الدراسات، إلا أنها اعتمدت على بيانات اصطناعية أو سيناريوهات محدودة، دون دمج آليات تكيف ديناميكية مع تغيّر السلوك الشبكي.

بالمقارنة مع هذه الأعمال، يتميّز العمل المقترح في هذه الدراسة بالتركيز على بيئة SDVN ذات حركية مستمرة وواقعية، مع بناء مجموعة بيانات جديدة، واستخدام مجموعة مدمجة من الميزات التدفقية السلوكية، وتقييم شامل لخوارزميات تعلّم آلي تقليدية ضمن إطار تصنيف متعدد الفئات، مع التركيز على مقياس F1–score بدل الاكتفاء بالدقة، مما يوفّر أساساً أكثر واقعية وموثوقية لتقييم أداء أنظمة كشف DDoS في شبكات العربات.

2. أهمية البحث وأهدافه:

مع التزايد المستمر في الاعتماد على شبكات العربات الذكية وأنظمة النقل المعتمدة على الاتصال، أصبح ضمان أمن شبكات العربات المعرفة بالبرمجيات (SDVN) أمراً بالغ الأهمية، ولا سيما في ظل طبيعتها الديناميكية واعتمادها على متحكم مركزي لإدارة الحركية. تُعد هجمات حجب الخدمة الموزعة (DDoS) من أخطر التهديدات التي تستهدف هذا النوع من الشبكات، لما لها من قدرة على تعطيل المتحكم المركزي، وإضعاف كفاءة إدارة التدفقات الشبكية، والتأثير المباشر على استقرار الخدمات الذكية. في هذا السياق، تبرز أهمية هذا البحث في مساهمته في تطوير آليات كشف فعالة وموثوقة لهجمات DDoS في بيئات SDVN، اعتماداً على التحليل السلوكي للتدفقات الشبكية وتقنيات التعلّم الآلي، بما ينسجم مع متطلبات البيئات الذكية الحديثة. تسهم هذه الدراسة في تعميق الفهم حول دور خوارزميات التعلّم الآلي في كشف الهجمات ضمن بيئات شبكية ديناميكية، مما يدعم بناء أنظمة دفاعية أكثر كفاءة وقابلية للتكيّف.

يهدف البحث بشكل رئيسي إلى:

- **تحليل سلوك الحركية في شبكات SDVN**: دراسة الخصائص السلوكية للتدفقات الشبكية في حالات الحركية الطبيعية والهجومية ضمن بيئة SDVN لاسلكية.
- **تقييم فعالية خوارزميات التعلّم الآلي:** تحليل أداء مجموعة من خوارزميات التعلّم الآلي التقليدية (RF, DT, KNN, SVM, LR, GNB) في تصنيف هجمات DDoS ضمن إطار تصنيف متعدد الفئات.

- **دراسة تأثير اختيار الميزات:** تقييم دور الميزات التدفقية الأساسية في تحسين دقة الكشف وتقليل تضخيم الأداء الناتج عن الاعتماد على ميزات مرتبطة بمنطق التصنيف الأصلي.
- **بناء خط أساس علمي موثوق:** توفير قاعدة مرجعية يمكن الاعتماد عليها لتقييم نماذج كشف أكثر تقدّماً، بما في ذلك نماذج التعلّم العميق أو النماذج الهجينة، في الدراسات اللاحقة.

3. طرائق البحث ومواده:

تم الاعتماد في هذه الدراسة على مجموعة بيانات واحدة تم توليدها خصيصاً لتمثيل بيئة شبكات العربات المعرفة بالبرمجيات (SDVN) اللاسلكية. جرى إنشاء مجموعة البيانات باستخدام محاكي Mininet-WiFi مع متحكم SDN من نوع Ryu، وذلك بهدف محاكاة بيئة حضرية ديناميكية تضم مركبات متحركة ونقاط وصول لاسلكية متعددة. شملت البيانات حركة مرور طبيعية وخمسة أنماط رئيسية من هجمات حجب الخدمة الموزعة (DDoS)، هي: SYN Flood (Bouyeddou et al., 2017)، UDP Flood (Khaing et al., 2020)، ICMP Flood (Zhang et al., 2020)، HTTP Flood (Jaafar et al., 2019)، و DNS Amplification (Moura et al., 2018)، بما يعكس سيناريوهات واقعية للتشغيل والهجوم ضمن شبكات SDVN.

بعد مرحلة جمع البيانات، خضعت مجموعة البيانات لسلسلة من خطوات المعالجة المسبقة لضمان جودتها وملاءمتها لعمليات التحليل والتصنيف. شملت هذه الخطوات توحيد تسميات الفئات الهجومية، وفحص البنية العامة للبيانات، والكشف عن القيم المفقودة وغير الفيزيائية الناتجة عن طبيعة الالتقاط اللحظي في الشبكات الديناميكية. تم التعامل مع القيم المفقودة باستخدام أساليب مناسبة تضمن اكتمال البيانات دون التأثير على توزيعها الإحصائي، كما جرى تحويل جميع الميزات المستخدمة إلى صيغ رقمية قابلة للمعالجة. بعد ذلك، أجرينا معايرة للبيانات باستخدام أساليب التطبيع المناسبة لتوحيد نطاق القيم ومنع الميزات ذات القيم الكبيرة من التأثير غير المتوازن على أداء النماذج. وفي مرحلة لاحقة، قُسمت البيانات إلى مجموعتي تدريب واختبار باستخدام تقسيم متوازن (Stratified Split) حيث يُحافظ هذا الأسلوب على التوزيع النسبي لكل فئة ضمن مجموعتي التدريب والاختبار، مما يضمن تمثيلاً متوازناً لجميع الفئات أثناء عملية التعلم والتقييم، ويسهم في تقديم تقدير أكثر موضوعية ودقة لأداء النماذج.

استناداً إلى نتائج التحليل الاستكشافي للبيانات، تم اختيار مجموعة من الميزات التدفقية الأساسية التي تُمثل السلوك الحقيقي للتدفقات الشبكية، شملت: معدل الحزم في الثانية Flow Packets/sec، معدل البايتات في الثانية Flow Bytes/sec، متوسط حجم الحزمة Flow Avg Packet Size داخل التدفق، الفاصل الزمني بين الحزم IPT، وطول الحزمة Packet Length. بعد ذلك، جرى تطبيق وتقييم مجموعة من خوارزميات التعلّم الآلي التقليدية على البيانات المعالجة، وهي: DT, RF, SVM, GNB, LR, KNN. تم اختيار هذه الخوارزميات لتمثيل طيف متنوع من أساليب التعلّم، بما يشمل النماذج الشجرية، الاحتمالية، والخطية.

تم تقييم أداء كل خوارزمية باستخدام مجموعة من المقاييس الإحصائية القياسية، شملت دقة التدريب والاختبار، معامل F1 (F1-Score)، وزمن التدريب والاختبار لقياس الكفاءة الزمنية للنماذج. جرى تنفيذ جميع مراحل المعالجة، التحليل، وبناء النماذج باستخدام لغة البرمجة Python (الإصدار 3.13)، مع الاعتماد على مكتبات التحليل والتعلّم الآلي القياسية.

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. المنهجية المقترحة:

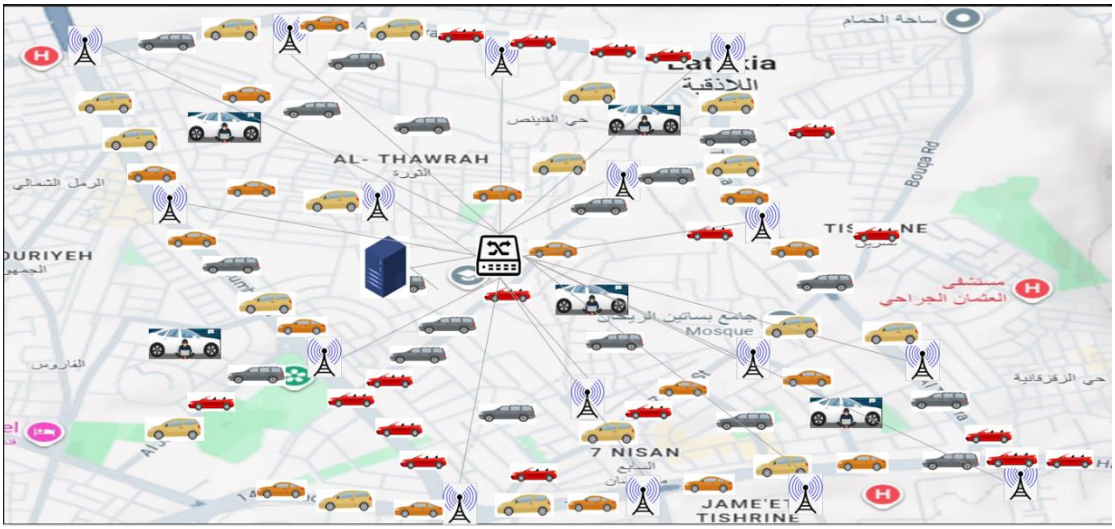
سنورد فيما يأتي تفاصيل قاعدة البيانات والخطوات العملية المطبقة والنتائج التي توصلنا إليها:

1.4 محاكاة بيئة SDVN لاسلكية واقعية:

تمت محاكاة بيئة شبكة عربات معرفة بالبرمجيات (SDVN) تمثل سيناريو حضري لشبكات العربات الذكية. تتكوّن الشبكة من محطات متنقلة تمثل المركبات تتصل ببنية تحتية من وحدات طرق جانبية (RSUs) موزعة داخل المدينة وعلى أطرافها، وترتبط جميعها عبر شبكة سلكية خلفية. أُديرت الشبكة بواسطة متحكم SDN من نوع Ryu باستخدام بروتوكول OpenFlow للتحكم المركزي في توجيه الحركية بين المركبات وRSUs والخوادم الداعمة لبروتوكولات TCP وUDP وHTTP وDNS.

تحركت العقد بسرعات بين 20–50 km/h وفق نموذج حركة عشوائي، مع انتقالها بين مناطق التغطية المختلفة لمحاكاة عمليات Handover وتغير جودة الاتصال في البيئات الحضرية. نُفذت المحاكاة ضمن منطقة حضرية مستمدة من جزء من مدينة اللاذقية بمساحة تقريبية 2000x2300 m^2. استخدمت RSUs الطرفية تردد 2.4GHz وفق معيار 802.11g، بينما اعتمدت RSUs الداخلية عالية الأداء تردد 5GHz وفق معيار 802.11ac كما يوضح الشكل (1).

استخدم نموذج الانتشار اللاسلكي logDistance بمعامل تلاشي 1.1 لمحاكاة فقد الإشارة، وتم ربط نقاط الوصول والخوادم السلكية بمبدل مركزي Open vSwitch للفصل بين طبقة النفاذ اللاسلكي والبنية السلكية الخلفية.



الشكل (1): السيناريو المستخدم في المحاكاة.

2.4 توليد الحركية الطبيعية وحركية DDoS:

تم توليد الحركية في بيئة SDVN وفق سيناريو زمني مضبوط امتد لمدة إجمالية قدرها 120 دقيقة، بهدف محاكاة سلوك الشبكة في حالتي التشغيل الطبيعي والتعرّض لهجمات حجب الخدمة الموزعة (DDoS). خُصِّصت الدقائق التسعون الأولى لتوليد الحركية الطبيعية على ثلاث مراحل زمنية متتالية، بحيث تعكس الزيادة التدريجية في عدد العربات النشطة وتنوّع البروتوكولات المستخدمة داخل الشبكة. في المرحلة الأولى (30–0 دقيقة)، تولّدت حركية طبيعية من 20 محطة متنقلة موزعة على بروتوكولات TCP (7) وUDP (7) وICMP (6). في المرحلة الثانية (60–30 دقيقة)، أُضيفت 15 محطة جديدة ليصبح التوزيع TCP (9)، UDP (9) ، ICMP (8)، HTTP (6)، و DNS (3). أما المرحلة الثالثة (90–60 دقيقة)، فقد أُضيفت 15 محطة إضافية ليصل العدد الكلي للمحطات ذات الحركية الطبيعية إلى 50 محطة، موزعة على TCP (12)، UDP (12)، ICMP (10)، HTTP (10)، و DNS (6).

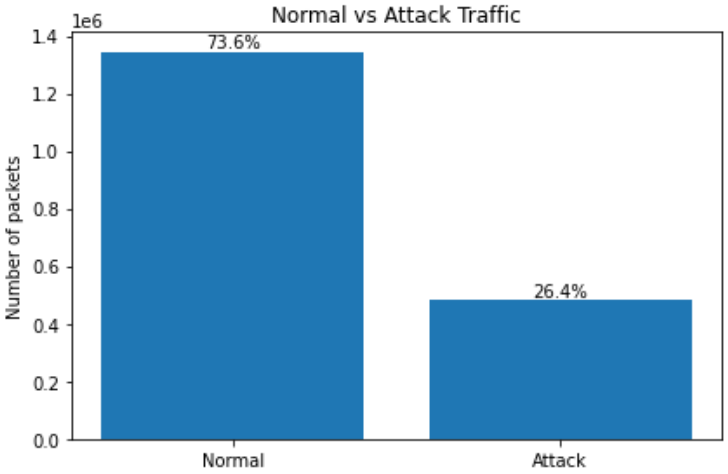
بعد انتهاء مرحلة التشغيل الطبيعي، خُصِّصت الدقائق الثلاثون الأخيرة (120–90 دقيقة) لتطبيق هجمات DDoS ضمن موجات زمنية متعاقبة، بحيث استغرقت كل موجة 5 دقائق. شملت الموجة الأولى (95–90 دقيقة) هجوم SYN Flood بمشاركة 5 محطات مهاجمة، تلتها الموجة الثانية (100–95 دقيقة) بهجوم UDP Flood، ثم الموجة الثالثة (105–100 دقيقة) بهجوم ICMP Flood، فالموجة الرابعة (110–105 دقيقة) بهجوم HTTP Flood، والموجة الخامسة (115–110 دقيقة) بهجوم DNS Amplification، مع ثبات عدد المحطات المهاجمة في كل موجة عند 5 محطات. في المرحلة الأخيرة (120–115 دقيقة)، نُفِّذت موجة هجومية متزامنة شملت جميع أنواع الهجمات السابقة في آن واحد بمشاركة 10 محطات مهاجمة، بهدف محاكاة سيناريو هجوم مركّب عالي الشدّة.

أتاح هذا التصميم الزمني المرحلي توليد مجموعة بيانات تمثّل بدقة الانتقال التدريجي من الحركية الطبيعية إلى الحالات الهجومية، مع المحافظة على وضوح الحدود الزمنية لكل نوع من الحركة، مما يوفر أساساً مناسباً لتحليل الخصائص السلوكية للتدفقات الشبكية وبناء نماذج كشف دقيقة لهجمات DDoS في بيئات SDVN الديناميكية.

3.4 تجميع البيانات وبناء Dataset:

جمعنا البيانات الناتجة عن محاكاة بيئة SDVN من خلال التقاط الحركية على مستوى الرزمة (Packet–level)، مع احتساب مؤشرات تراكمية على مستوى التدفق (Flow–level) في الزمن الحقيقي. جرى تخزين البيانات ضمن ملف بصيغة CSV، بحيث يمثّل كل سجل رزمة واحدة مرفقةً بمجموعة من الخصائص الشبكية المستخرجة من طبقات الشبكة والنقل والتطبيق، إضافةً إلى إحصائيات التدفق الذي تنتمي إليه الرزمة في لحظة الالتقاط. يتيح هذا الأسلوب دمج الخصائص اللحظية للرزم مع السلوك التراكمي للتدفقات، مما يوفر تمثيلاً أكثر واقعية للحركية الشبكية.

بلغ الحجم النهائي لمجموعة البيانات بعد انتهاء جميع مراحل المحاكاة 1,827,265 سجلاً، توزّعت بين 1,345,565 سجلاً لحركة طبيعية (73.6%) و481,700 سجلاً لحركة هجومية (26.4%). يعكس هذا التوزيع سيناريو تشغيلياً واقعياً تميل فيه الشبكة إلى الحالة الطبيعية مع وجود نسبة ملحوظة من الهجمات. يوضّح الشكل (2) التوزيع العام بين الحركة الطبيعية والهجومية



الشكل (2): نسبة الحركة الطبيعية والهجومية ضمن Dataset المولدة.

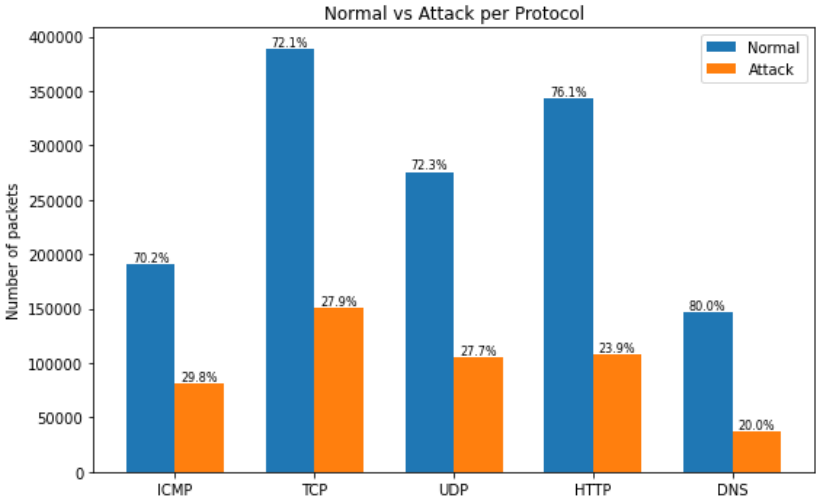
في حين يبيّن الشكل (3) توزيع هذه الحركة على مستوى البروتوكولات المختلفة (ICMP، TCP، UDP، HTTP، DNS)، حيث يعكس التوزيع النسبي والكمّي لحركة المرور الطبيعية والهجومية ضمن بيئة SDVN المدروسة. يظهر بوضوح أن جميع البروتوكولات يغلب عليها الطابع الطبيعي، إذ تتراوح نسبة الحركة الطبيعية بين (70%–80%)، مقابل نسب هجومية تقع ضمن المجال (20%–30%)، وهو ما يشير إلى توازن مقصود في بناء مجموعة البيانات بحيث تمثل سيناريو شبه واقعي دون الانحياز المفرط لأي فئة.

وعلى المستوى الكمي، يلاحظ أن بروتوكولي TCP وHTTP يسجلان أعلى حجم مطلق من الحركة مقارنة ببقية البروتوكولات، وهو أمر متوقع نظراً لاعتمادهما في معظم تطبيقات الشبكات الحضرية وخدمات الإنترنت (مثل نقل البيانات، والتصفح، والخدمات السحابية). في المقابل، تظهر بروتوكولات مثل DNS وICMP أحجاماً أقل نسبياً، إلا أنها تحتفظ بنفس النمط النسبي بين الحركة الطبيعية والهجومية، مما يعكس توزيعاً متوازناً عبر مختلف طبقات البروتوكولات.

تُبرز هذه النتائج دلالات مهمة على مستوى تحليل السلوك الشبكي، حيث أن ارتفاع حجم الحركة في بروتوكولات TCP وHTTP يجعلها أكثر عرضة للاستهداف بهجمات DDoS، خاصة الهجمات القائمة على الاستنزاف الحجمي (Volumetric Attacks) أو استغلال آليات الاتصال (مثل SYN Flood و HTTP Flood). من جهة أخرى، فإن البروتوكولات ذات الحجم الأقل مثل DNS قد تُستخدم في هجمات تضخيم (Amplification Attacks)، مما يعني أن خطورتها لا ترتبط بالحجم الظاهر فقط بل بطبيعة الاستخدام.

إضافة إلى ذلك، فإن تقارب النسب بين الحركة الطبيعية والهجومية عبر جميع البروتوكولات يشير إلى أن عملية الكشف لا يمكن أن تعتمد على الحجم المطلق للتدفق فقط، بل يجب أن تستند إلى تحليل سلوكي دقيق للميزات الإحصائية (مثل معدل الحزم، ومعدل البايتات، ومتوسط حجم الرزمة)، حيث أن الأنماط الهجومية قد تظهر ضمن نفس النطاقات الكمية ولكن بسلوك زمني مختلف.

بناءً على ذلك، يؤكد هذا التوزيع أهمية اعتماد نماذج كشف تأخذ بعين الاعتبار الخصائص الخاصة بكل بروتوكول (Protocol-aware Detection)، بدلاً من استخدام عتبات موحدة لجميع أنواع الحركية، خاصة في بيئات SDVN الديناميكية التي تتأثر بطبيعة الحركة اللاسلكية وتغيراتها الزمنية.



الشكل (3): توزع الحركية الطبيعية والهجومية لكل بروتوكول.

تضمنت مجموعة البيانات مجموعة واسعة من الميزات التي تمثل خصائص الرزم والتدفقات، شملت معلومات زمنية، وعناوين IP، وأرقام المنافذ، ونوع البروتوكول، وطول الرزمة، وأعلام TCP، إضافةً إلى مؤشرات تدفقية مثل عدد الرزم والبايتات المتراكمة والفاصل الزمني بين الرزم. يوضّح الجدول (2) قائمة الميزات المستخدمة ووصف كل منها، والتي شكّلت الأساس لعمليات التحليل الإحصائي وبناء نماذج التعلّم الآلي.

الجدول (2): الميزات الموجودة ضمن مجموعة البيانات المولدة.

اسم الميزة	النوع	الوصف
Timestamp	فئوي	الطابع الزمني لتوقيت استقبال الرزمة في معالجتها بتنسيق تاريخ/وقت
Source IP	فئوي	عنوان IP الخاص بالمصدر الذي أرسل الرزمة
Destination IP	فئوي	عنوان IP الخاص بالهدف الذي استقبل الرزمة
Source Port	رقمي	رقم منفذ المصدر
Destination Port	رقمي	رقم منفذ الهدف
ProtocolNum	رقمي	رقم البروتوكول في ترويسة IP
AppProto	فئوي	البروتوكول على مستوى التطبيق حيث يستنتج من رقم المنفذ وقيمة ProtocolNum
Packet Length	رقمي	طول الرزمة بالبايت
Flags	فئوي	حقول الأعلام الخاصة بـ TCP
Window Size	رقمي	حجم نافذة TCP للرزمة الحالية
CheckSum	رقمي	قيمة حقل التحقق في ترويسة TCP/UDP
Bytes	رقمي	عدد البايتات المتراكمة ضمن التدفق نفسه منذ أول رزمة حتى الحالية
Packets	رقمي	إجمال عدد الرزم المتراكمة ضمن نفس التدفق حتى لحظة الرزمة الحالية
Inter-packet Time (IPT)	رقمي	الفاصل الزمني بين الرزمة الحالية والرزمة السابقة ضمن التدفق نفسه (بالثانية)

Flow Packet/sec	رقمي	معدل الرزم في الثانية للتدفق محسوباً على كامل مدة التدفق منذ أول رزمة حتى اللحظة الحالية
Flow Bytes/sec	رقمي	معدل البايتات في الثانية محسوباً عل كامل مدة التدفق
Flow Avg Packet Size	رقمي	متوسط حجم الرزمة ضمن التدفق نفسه حتى اللحظة الحالية
Packet Type	فئوي	نوع الرزمة

اعتمدت عملية حساب الميزات التدفقية على تعريف مفتاح تدفق مكوّن من (عنوان المصدر، عنوان الوجهة، البروتوكول التطبيقي، منفذ المصدر، منفذ الوجهة). وبالاعتماد على زمن أول وآخر رزمة داخل كل تدفق، تم حساب معدل الرزم في الثانية (Flow Packets/sec)

$$Flow\ Packets\ /sec\ = \frac{Packets}{Flow\ Duration\ (seconds)} \qquad (1)$$

معدل البايتات في الثانية (Flow Bytes/sec)

$$Flow\ Bytes\ /sec\ = \frac{Bytes}{Flow\ Duration\ (seconds)} \qquad (2)$$

متوسط حجم الرزمة (Flow Avg Packet Size)

$$Flow\ Avg\ Packet\ Size = \frac{Bytes}{Packets} \qquad (3)$$

تُمكّن هذه المؤشرات من توصيف السلوك الزمني والإحصائي للتدفقات، وتساعد على التمييز بين الأنماط الطبيعية والهجومية (Santos da Silva et al., 2015).

أخيراً، جرى وسم كل سجل ضمن مجموعة البيانات اعتماداً على حقل Packet Type الناتج عن البرنامج المكتوب بلغة Python والخاص بالالتقاط، والذي يستند إلى مزيج من تحليل أعلام TCP ومؤشرات التدفق ومقارنتها مع عتبات ديناميكية مخصّصة لكل بروتوكول. وفّرت هذه الآلية مجموعة بيانات منظّمة وغنية تمثّل بدقة السلوك الشبكي في حالات التشغيل الطبيعي والتعرّض لهجمات DDoS، وشكّلت أساساً موثوقاً لمراحل التحليل اللاحقة وتدريب نماذج التعلّم الآلي.

4.4 تنظيف البيانات والتحقق من جودتها:

بعد تجميع البيانات خضعت مجموعة البيانات لمرحلة تنظيف وفحص جودة. شملت المرحلة الأولى توحيد تسميات الهجمات ضمن الحقل Packet Type، حيث دُمجت التسميات المتقاربة مثل DNS Flood و DNS Amplification Attempt ضمن فئة DNS Amplification، كما دُمجت العينات المصنفة TCP Anomaly ضمن فئة SYN Flood.

أظهر الفحص البنيوي أن مجموعة البيانات تضم 1,827,265 سجلاً موزعة على 18 حقلاً تتضمن معلومات زمنية، وعناوين IP، وأرقام المنافذ، ونوع البروتوكول، وخصائص الرزم، إضافة إلى مؤشرات تدفقية مثل Flow Packets/sec وFlow Bytes/sec وFlow Avg Packet Size. كما تبيّن أن معظم الحقول مكتملة، بينما ظهرت قيم مفقودة في بعض حقول TCP مثل Flags وWindow Size بنسبة 45.78% نتيجة عدم وجودها في بروتوكولات أخرى، إضافة إلى 14.87% في CheckSum و6.84% في Inter-packet Time.

كشف التحليل الإحصائي وجود قيم شاذة غير متوافقة مع القيود الفيزيائية لشبكات IEEE 802.11 مثل أطوال رزم تتجاوز 1500 بايت أو قيم غير منطقية للفاصل الزمني بين الرزم. لذلك طُبّقت مرحلة تنظيف تعتمد

قيوداً فيزيائية شملت حذف السجلات التي تتجاوز فيها Packet Length أو Flow Avg Packet Size قيمة 1500 بايت، واستبعاد القيم التي تتجاوز 300 ثانية في IPT، إضافة إلى إزالة معدلات التدفق غير الواقعية.

أسفرت عملية التنظيف عن حذف 246,182 سجلاً، ليصبح الحجم النهائي لمجموعة البيانات 1,581,083 سجلاً. وأظهر فحص الموثوقية أن البيانات بعد التنظيف ما تزال تحتفظ بتوزيع منطقي للحركة الشبكية بنسبة 76.92% حركة طبيعية مقابل 23.08% حركة هجومية.

5.4 اختيار الميزات (Feature Selection)

استند اختيار الميزات في هذه الدراسة إلى نتائج التحليل الاستكشافي للبيانات (EDA) الذي أُجري على مجموعة البيانات بعد مرحلة التنظيف. تم تحليل التوزيعات الإحصائية لعدد من الميزات البنيوية والزمنية ومقارنة سلوكها بين الحركة الطبيعية وهجمات DDoS بهدف تحديد الخصائص الأكثر قدرة على التمييز بين الفئتين.

أظهرت نتائج الإحصاءات الوصفية وجود فروق واضحة بين الحركة الطبيعية والهجومية في عدد من المؤشرات المرتبطة بكثافة الإرسال وحجم الرزم والسلوك الزمني للتدفّقات. فعلى سبيل المثال، ارتفع الوسيط لميزة Flow Packets/sec من نحو 3.76 في الحركة الطبيعية إلى 248.93 في الحركة الهجومية، كما ارتفع الوسيط لميزة Flow Bytes/sec من 270.57 إلى 57,677.32. كذلك أظهرت ميزة Packet Length زيادة في الوسيط من 95 بايت في الحركة الطبيعية إلى 206 بايت في الحركة الهجومية، إضافة إلى اختلافات واضحة في التوزيع الإحصائي لكل من Inter-Packet Time (IPT) و Flow Avg Packet Size.

تشير هذه النتائج إلى أن الميزات المرتبطة بمعدل الإرسال، حجم الرزم، والبنية الزمنية للتدفّقات تُعد الأكثر حساسية للتغيرات التي تُحدثها هجمات DDoS. بناءً على ذلك، تم اختيار خمس ميزات تدفّقية أساسية لاستخدامها في نماذج التعلّم الآلي، وهي: Flow Packets/sec، Flow Bytes/sec، Flow Avg Packet Size، Inter-Packet Time (IPT)، وPacket Length.

يوضح الجدول (3) مقارنة إحصائية مختصرة لهذه الميزات بين الحركة الطبيعية والهجومية استناداً إلى نتائج التحليل الاستكشافي للبيانات.

الجدول (3): مقارنة الميزات من ناحية الوسيط.

الميزة	الوسيط للحركية الطبيعية	الوسيط للحركية الهجومية	الدلالة
Flow Packet/sec	3.76	248.93	ارتفاع كبير في معدل الرزم أثناء الهجوم
Flow Bytes/sec	270.57	57,677.32	زيادة كبيرة في معدل نقل البيانات
Packet Length	94 B	206 B	تغير واضح في بنية الرزم
IPT	0.01 s	0.72 s	تغير في النمط الزمني للتدفقات
Flow Avg Packet Size	98 B	115 B	اختلاف في متوسط حجم الرزم

6.4 نتائج وتقييم المنهجية المقترحة

يهدف هذا القسم إلى تقييم فعالية المخطط المقترح لكشف هجمات DDoS في بيئة SDVN من خلال مهمة تصنيف متعددة الفئات (10 فئات) تشمل أنماط الحركة الطبيعية والهجومية، وهو إعداد يعكس بشكل أقرب الواقع التشغيلي مقارنة بالتصنيفات المبسطة.

اعتمدت التجربة على مجموعة بيانات تضم 1,581,083 عينة، قُسمت بنسبة 70% للتدريب و30% للاختبار باستخدام Stratified Sampling. تم تدريب ستة نماذج تعلم آلي باستخدام خمس ميزات تدفقية أساسية، ويعرض الجدول (4) نتائج الأداء.

الجدول (4): نتائج تطبيق المصنفات على مجموعة البيانات.

النموذج	دقة التدريب	دقة الاختبار	Macro F1	Weighted F1	زمن التدريب (ثانية)	زمن التنبؤ (ثانية)
RF	99.76%	98.29%	96.78%	98.29%	149.04	3.18
DT	99.76%	97.77%	95.73%	97.77%	10.66	0.096
KNN	98.19%	97.46%	95.35%	97.45%	4.13	40.43
LR	63.8%	63.9%	65%	59.9%	169.74	0.086
Linear SVM	56.6%	56.6%	48.6%	49.2%	52.71	0.064
NB	56.3%	56.3%	57.8%	49.7%	0.26	0.51

تحليل الأداء العام للنماذج

-أفضل أداء عام: حقق نموذج Random Forest (RF) أعلى دقة اختبار (98.29%) وأعلى Macro F1 (96.78%)، مما يدل على قدرة عالية على التعميم والتوازن بين جميع الفئات.

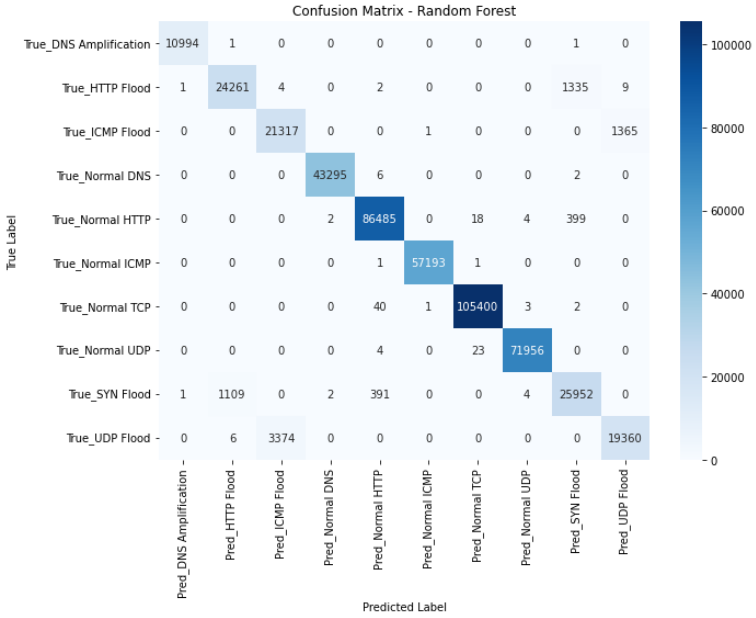
-النماذج الشجرية (RF, DT): أظهرت أداءً متفوقاً بفضل قدرتها على تمثيل العلاقات غير الخطية في بيانات التدفق.

-النماذج الخطية والاحتمالية (LR, SVM, NB): سجلت أداءً ضعيفاً، مما يشير إلى عدم ملاءمتها لطبيعة البيانات الشبكية المعقدة.

-زمن التنفيذ:

- NB و SVM الأسرع في التنبؤ لكن بدقة منخفضة.
- KNN بطيء جداً في التنبؤ، مما يجعله غير مناسب للزمن الحقيقي.
- RF يحقق توازناً جيداً بين الدقة والزمن، ما يجعله الخيار الأنسب عملياً.

تُظهر مصفوفة الالتباس الخاصة بنموذج Random Forest كما في الشكل (4) أن معظم التصنيفات كانت دقيقة،



الشكل (4): مصفوفة الالتباس الخاصة بالنموذج الأفضل RF.

حيث تركزت القيم العالية على القطر الرئيسي، مما يدل على قدرة النموذج على التمييز بين الأنواع المختلفة من الحركة الشبكية بشكل عام. ومع ذلك، لوحظ وجود التباسات محددة بين بعض الأصناف، خاصةً بين أنواع الهجمات التي تتشارك سلوكاً شبكياً متقارباً. على سبيل المثال، ظهر التباس واضح بين هجمات SYN Flood وHTTP Flood، حيث تم تصنيف عدد ملحوظ من تدفقات SYN Flood على أنها HTTP Flood والعكس بالعكس. يُعزى ذلك إلى أن كلا النوعين يتميزان بمعدلات مرتفعة لتدفقات الحزم وعدد كبير من الجلسات، مما يجعل الفصل بينهما صعباً عند الاعتماد فقط على ميزات إحصائية عامة على مستوى التدفق مثل معدل الحزم وحجمها، دون تضمين خصائص بروتوكولية دقيقة كأعلام TCP أو نسبة SYN/ACK.

كذلك، سُجّل التباس بين هجمات ICMP Flood وUDP Flood، وهو أمر متوقع نظراً لأن كلا الهجومين يتسمان بطبيعة عديمة الحالة (stateless) ومعدلات إرسال مرتفعة، إضافةً إلى تشابه أحجام الحزم في كثير من الحالات. هذه الخصائص تجعل الأنماط السلوكية لهذين النوعين متقاربة من منظور الميزات المستخدمة، مما يحد من قدرة النموذج على الفصل التام بينهما. بشكل عام، تشير هذه الالتباسات إلى أن صعوبة التصنيف لا تعود إلى ضعف النموذج بحد ذاته، وإنما إلى التشابه السلوكي بين بعض أنواع الهجمات عند تمثيلها بعدد محدود من الميزات الإحصائية.

7.4 مقارنة مع الدراسات المرجعية

تُظهر الدراسات المرجعية السابقة تنوعاً في الأساليب المستخدمة لكشف هجمات DDoS في البيئات المعرفة بالبرمجيات، إلا أنها تختلف من حيث واقعية بيئة التجربة ونوع البيانات المستخدمة ومنهجية التقييم. يوضّح الجدول (5) مقارنة بين أهم هذه الدراسات والعمل الحالي.

الجدول (5): مقارنة مع الدراسات المرجعية.

الدراسة	بيئة التجربة	نوع البيانات	النموذج المستخدم	القيود في الدراسة	مقارنة بالعمل الحالي
[12]	شبكات SDN تقليدية	مجموعات بيانات عامة	RF, KNN, SVM	عدم وجود حركية للشبكة وعدم تمثيل بيئة شبكات العربات	العمل الحالي يعتمد بيئة SDVN ديناميكية مع حركية مركبات واقعية
[7]	بيئة SDN مخبرية	بيانات عامة	ML مع SelectKBest	البيانات غير واقعية ولا تمثل سلوك الشبكات المتحركة	الدراسة الحالية تولد Dataset مخصصة لشبكات SDVN
[6]	شبكات SDN	بيانات تجريبية	نماذج DL	تعقيد حسابي مرتفع وصعوبة التطبيق في الزمن الحقيقي	العمل الحالي يحقق دقة مرتفعة باستخدام نماذج ML أخف حسابياً
[4]	SDVN جزئية	تحليل تدفقات	ML	عدم وجود حركية مستمرة وعدم استخدام عتبات ديناميكية	الدراسة الحالية تعتمد سيناريو حركي كامل مع تغير تدريجي في الحركة والهجمات
[1]	شبكات IoV	بيانات اصطناعية	نموذج هجين متقدم	اعتماد بيانات اصطناعية	العمل يستخدم Dataset مولدة من محاكاة حضرية واقعية
[13]	IoV	بيانات محاكاة	DL متعدد الوسائط	تعقيد النموذج وعدم التركيز على ميزات تدفقية بسيطة	تعتمد الدراسة الحالية ميزات تدفقية سلوكية تحقق دقة عالية مع تعقيد منخفض
الدراسة الحالية	بيئة SDVN لاسلكية ديناميكية باستخدام Mininet-WiFi و Ryu	Dataset مولدة خصيصاً (أكثر من ١,٥ مليون سجل)	DT, RF, KNN, LR, SVM, NB		تحقيق دقة اختبار 98.29% باستخدام RF مع تصنيف متعدد الفئات وتمثيل واقعي لسلوك الشبكة

الاستنتاجات والتوصيات:

تناولت هذه الدراسة مشكلة كشف هجمات حجب الخدمة الموزعة (DDoS) في بيئة شبكات SDVN من خلال تصميم وتقييم مخطط كشف قائم على تحليل التدفقات الشبكية باستخدام نماذج التعلّم الآلي التقليدية. تم بناء بيئة محاكاة لاسلكية تحاكي سيناريوهات المدن الذكية، وتوليد حركة طبيعية وخمسة أنماط هجومية، ثم معالجة البيانات وتنفيذ تصنيف متعدد الفئات.

أظهرت النتائج ما يلي:

-كفاية مجموعة مدمجة من خمس ميزات تدفقية في تمثيل السلوك الشبكي وتمكين النماذج من التمييز الفعال بين الحركة الطبيعية والهجومية.

-تفوق النماذج غير الخطية، وخاصة Random Forest، من حيث الدقة والتوازن بين الفئات.

-تحقيق Decision Tree أداءً قريباً مع زمن تنبؤ منخفض، مما يجعله مناسباً للتطبيقات الزمن الحقيقي.

-محدودية أداء النماذج الخطية والاحتمالية في تمثيل التعقيد السلوكي لهجمات DDoS.

-استمرار التحدي في التمييز بين الهجمات المتقاربة سلوكياً (مثل UDP Flood و ICMP Flood)، مما يعكس واقعية السيناريو التجريبي.

تشير هذه النتائج إلى أن الاعتماد على ميزات تدفقية سلوكية مع نماذج تعلم غير خطية يشكّل أساساً فعالاً لبناء أنظمة كشف DDoS في بيئات SDVN، مع ضرورة تحقيق توازن بين الدقة والكفاءة الزمنية وفق متطلبات التطبيق. كآفاق مستقبلية، يُقترح توسيع العمل عبر استخدام نماذج تعلم عميق أو هجينة، وتقييم الأداء في بيئات زمن حقيقي، إضافةً إلى دراسة قابلية التعميم على بيانات حقيقية وسيناريوهات واسعة النطاق.

المراجع:

ABABSA,F.; DERDOUR,M.; BOUKHALFA,K.; BOUSHABA,A.; BOUKERRAM,A., 2025, "*Deep multimodal learning for real time DDoS attacks detection in Internet of Vehicles". IEEE Transactions on Intelligent Transportation Systems.*

ASLAM,S.; SRIVASTAVA,S.; GORE,M.M., 2025, *"Security and deployment challenges in software-defined vehicular networks ".* Computer Networks, Netherlands, Vol.250, 110831.

BATOOL,S.; ASLAM,M.; AKPOKODJE,E.; JILANI,S.F., 2025, *"A comprehensive review of DDoS detection and mitigation in SDN environments: Machine learning, deep learning, and federated learning perspectives".* Electronics, Switzerland, Vol.14, No.21, 4222.

BABBAR,H.; RANI,S.; DRISS,M., 2024, *"Effective DDoS attack detection in software-defined vehicular networks using statistical flow analysis and machine learning".* PLOS ONE, U.S.A., Vol.19, No.12, e0314695.

BOUYEDDOU,B.; HARROU,F.; SUN,Y.; KADRI,B., 2017, *"Detecting SYN flood attacks via statistical monitoring charts: A comparative study".* in Proc. ICEE-B, Algeria.

ELUBEYD,H.; YILTAS KAPLAN,D., 2023, *"Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software defined networks".* Applied Sciences, Switzerland, Vol.13, No.6, 3828.

HAKEEM,A.; ATTIAH,A., 2024, *"Machine Learning-based Approach for Detecting DDoS Attacks in Software Defined Networks".* International Journal of Computer Applications, Vol.186, No.43, 1–9.

HILL,W.; ACQUAAH,Y.T.; MASON,J.; LIMBRICK,D.; TEIXEIRA-POIT,S.; COATES,C.; ROY,K., 2024, *"DDoS in SDN: A review of open datasets, attack vectors and mitigation strategies".*

JAAFAR,G.A.; ABDULLAH,S.M.; ISMAIL,S., 2019, *"Review of recent detection methods for HTTP DDoS attack".* Journal of Computer Networks and Communications, Vol.2019, 1–10.

KHAING,M.S.; THANT,Y.M.; TUN,T.; HTWE,C.S.; THWIN,M.M.S., 2020, "IoT botnet detection mechanism based on UDP protocol". in Proc. IEEE ICCA.

MOURA,G.C.M.; HEIDEMANN,J.; MÜLLER,M.; SCHMIDT,R.; DAVIDS,M., 2018, "When the dike breaks: Dissecting DNS defenses during DDoS". in Proc. IMC.

NADEEM,M.W.; GOH,H.G.; PONNUSAMY,V.; AUN,Y., 2022, "DDoS Detection in SDN using Machine Learning Techniques". Computers, Materials & Continua, Vol.71, No.1, 771–789.

SARVADE,R.; PATEL,M.; KHAN,A.; AL QAHTANI,S., 2025, "A hybrid classical quantum neural network model for DDoS attack detection in software defined vehicular networks". Arabian Journal for Science and Engineering, Vol.50, No.2, 1234–1248.

SANTOS DA SILVA,A.; MACHADO,C.C.; BISOL,R.V.; GRANVILLE,L.Z.; SCHAEFFER-FILHO,A., 2015, "Identification and Selection of Flow Features for Accurate Traffic Classification in SDN". in Proc. IEEE NCA, 134–141.

ZHANG,M.; LI,G.; WANG,S.; LIU,C.; CHEN,A.; HU,H.; GU,G.; LI,Q.; XU,M.; WU,J., 2020, "Poseidon: Mitigating volumetric DDoS attacks with programmable switches". in Proc. NDSS.