Applying Machine Learning to Detect DDoS Attacks in SD-VANET Networks

Dr. Bassam Hasan•

(Received 7 / 10 / 2024. Accepted 24 / 11 / 2024)

□ ABSTRACT □

Vehicular Ad Hoc Network (VANET) is a modern technology that integrates next-generation wireless network capabilities into vehicles. Integrating Software-Defined Networking (SDN) with VANETs is a significant step towards developing intelligent vehicular networks. This new architecture offers innovative solutions to VANET challenges in various fields, especially in security.Using machine learning to detect Distributed Denial of Service (DDoS) attacks in Software-Defined VANETs (SD-VANET) is a modern and effective technique. This approach relies on analyzing network traffic patterns and detecting abnormal behaviors that indicate DDoS attacks. Machine learning algorithms can quickly and accurately identify these patterns, helping to take preventive measures to protect the network.

In this research, an SDN-VANET environment was created using the Mininet-WiFi emulator, with the Ryu controller providing software components and APIs that facilitate developers in creating new applications for network management and control. Statistical information extracted from flow tables was used to detect DDoS attacks targeting controllers in the SDN-VANET environment. The dataset used to train the machine learning model was obtained from the experimentally designed SD-VANET architecture, and the best-performing parameters for the SVM classifier were used during the training phase, resulting in high accuracy.

Keywords: Vehicular Ad Hoc Network, Software Defined Networks. Distributed denial of service attack

• **Ph.D., Department of Communication and Electronics, Faculty of mechanical and electrical engineering, Tishreen University, Lattakia, Syria. Email: bassam.a.hasan@tishreen.edu.sy**

تطبيق التعلم الآلي لكشف هجمات حجب الخدمة الموزعة في شبكات SD-VANET

د. بسام حسن •

(تاريخ الإيداع 7 / 10 / 2024. قُبِل للنشر في 24/ 11 / 2024)

□ ملخّص □

شبكات العربات المتنقلة VANET (vehicular ad-hoc network) تقنية حديثة تدمج إمكانات الجيل التالي من الشبكات اللاسلكية في المركبات. يعد دمج الشبكات المعرفة بالبرمجيات SDN (Software-defined networking) مع VANET خطوة مهمة نحو تطوير شبكات المركبات الذكية. تقدم هذه البنية الجديدة حلولًا مبتكرة لتحديات VANET في مختلف المجالات، وخاصة في المجال الأمني. يُعد استخدام التعلم الآلي في كشف هجمات حجب الخدمة الموزعة DDoS في شبكات المركبات المعرفة برمجياً SD-VANET من التقنيات الحديثة والفعالة. تعتمد هذه التقنية على تحليل أنماط حركة البيانات في الشبكة واكتشاف السلوكيات غير الطبيعية التي تشير إلى وجود هجمات DDoS (Distributed Denial of Service). تتعرف خوارزميات التعلم الآلي بسرعة ودقة على الأنماط غير الطبيعية، مما يساعد في اتخاذ الإجراءات الوقائية اللازمة لحماية الشبكة.

في هذه الورقة البحثية، تم إنشاء بيئة SDN-VANET باستخدام المحاكي Mininet-WiFi، مع استخدام المتحكم Ryu الذي يوفر مكونات برمجية وواجهات برمجة تطبيقات تسهل على المطورين إنشاء تطبيقات جديدة لإدارة الشبكة والتحكم فيها. تم استخدام المعلومات الإحصائية المستخلصة من جداول التدفق لكشف هجمات DDoS التي تستهدف المتحكمات في بيئة SDN-VANET. تم الحصول على مجموعة البيانات المستخدمة لتدريب نموذج التعلم الآلي من بنية SD-VANET المصممة تجريبيًا، وتم استخدام أفضل المعلمات أداءً لمصنف التعلم الآلي SVM أثناء مرحلة التدريب، مما أدى إلى تحقيق درجة دقة عالية.

الكلمات المفتاحية: شبكات العربات المتنقلة، الشبكات المعرفة بالبرمجياتش. هجوم حجب الخدمة الموزع.

• **دكتوراه، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية سورية.**
bassam.a.hasan@tishreen.edu.sy

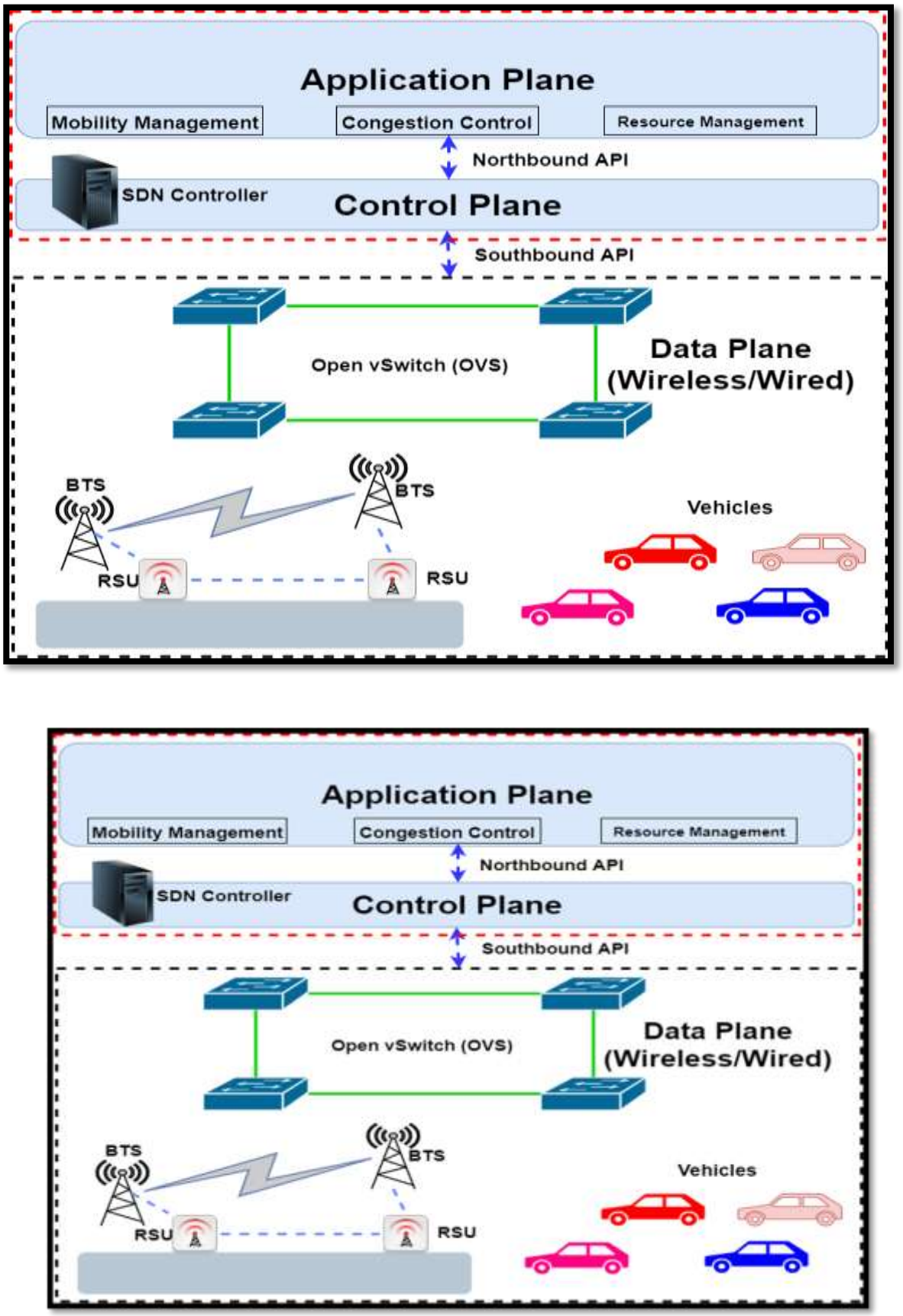
مقدمة:

في المستقبل القريب، من المتوقع أن يكون هناك زيادة هائلة في عدد المركبات المتصلة، حيث ستكون أكثر بألف مرة مما هي عليه اليوم، مع متطلبات متنوعة لربط مختلف الخدمات والتطبيقات غير المتجانسة والمخصصة عبر الإنترنت. تعمل الشبكات المعرفة بالبرمجيات (SDN) على سد الفجوة بين متطلبات تطبيقات المركبات والقيود المفروضة على نشر شبكة المركبات. توفر VANET المدعومة بتقنية SDN وحدة تحكم لتحديد قواعد إعادة توجيه البيانات للمبدلات في مستوى البيانات، مما يسهل إدارة شبكة المركبات المعقدة والديناميكية بشكل أبسط وأسرع. يتم تنفيذ SDN باستخدام OpenFlow [1]، وهو بروتوكول اتصال بين وحدة التحكم ووكيل توجيه البيانات لتوجيه البيانات عبر جداول التدفق.

الشبكة المعرفة بالبرمجيات (SDN) هي بنية شبكة جديدة أكثر قابلية للإدارة والتكيف والديناميكية والبرمجة. على الرغم من أن مستوى التحكم منفصل عن مستوى التوجيه وقابل للبرمجة بشكل مباشر، إلا أن ذلك يجعل الشبكة سريعة وسهلة الإدارة. تعمل تقنية SDN على زيادة قدرة الشبكة وتخفيض زمن تكوينها وإدارة الموارد لميزاتها القابلة للبرمجة. البنية الحديثة، التي تم إنشاؤها عن طريق تكييف وتكامل نموذج SDN مع VANET التقليدي تسمى SD-VANET[2,3]. التي تسمح بتوسيع نطاق الشبكة بسهولة وإدارة أكثر مرونة للشبكة. ولكن على الرغم من المزايا المتنامية لبنية SD-VANET، إلا أنها عرضة أيضا لتهديدات الهجمات الإلكترونية مثل حجب الخدمة الموزع DDoS. على الرغم من أن SD-VANET يتمتع بالعديد من المزايا. ولكن وحدة التحكم، التي تدير الشبكة بأكملها، هي هدف للمهاجمين. لذلك تشكل هجمات DDoS التي يمكنها تعطيل وحدة التحكم تهديدا كبيرا لبنية هذه الشبكات. لذلك يجب اتخاذ الاحتياطات اللازمة ضد الهجمات الإلكترونية التي ستؤثر على كفاءة النظام وأمنه. بدون اتخاذ هذه الاحتياطات، إذا تعرضت بنية الشبكة لهجوم إلكتروني، فقد تحدث العديد من العواقب غير المرغوب فيها، مثل أضرار البنية التحتية وتعريض حياة الإنسان للخطر.

تتكون بنية SD-VANET المقترحة والموضحة بالشكل (1) من المكونات التالية. (أ) مستوى التحكم: وحدة تحكم SDN الموحدة منطقيًا والتي توفر وظائف التحكم في الشبكة بأكملها. تتواصل وحدة التحكم مع أجهزة الشبكة في مستوى البيانات ومع التطبيق. (ب) مستوى البيانات: يتكون مستوى البيانات من المركبات (أي العقد المتنقلة اللاسلكية التي تدعم SDN) و RSU (أي العقد الثابتة التي تدعم SDN) التي تستقبل رسالة التحكم من مستوى التحكم. تحتوي كل عقدة لاسلكية ممكّنة لـ SDN على وكيل محلي، يسمى وكيل SDN. يتم استخدام وكيل SDN للتواصل مع وحدة التحكم.

يمتلك المبدل في هذه الشبكات جدولاً أو أكثر يسمى جدول التدفق (flow table) ، تبعا لمواصفات OpenFlow لا يقوم المبدل بمعالجة الطرود الواردة إليه، انما يقوم بالبحث عن تطابق بين الطرد الوارد وإحدى المدخلات الموجودة ضمن جدول التدفق ، فعندما لا يجد تطابقاً، يقوم بإرسال رسالة (Packet_In) إلى المتحكم لطلب الإرشادات ، حيث يقوم المتحكم بمعالجة المعطيات وإصدار الإجراء اللازم اتخاذه من قبل المبدل بشأن هذا الطرد ، وبالتالي اذا تلقى المبدل عدد كبير من الطرود الواردة في وقت قصير والتي لا يجد لها تطابقا ضمن جدول التدفق سيتعين على وحدة التحكم التعامل مع كمية هائلة من رسائل (Packet_In) مما يؤدي إلى استنزاف موارده وشل حركته ، وهذا ما يمكننا تخيله في حال تعرض الشبكة المعرفة برمجيا لهجمات حجب الخدمة الموزعة (DDoS) [4,5].



الشكل (1). شبكة SD-VANET

أهمية البحث وأهدافه:

تعدّ بيئة شبكات العربات المعتمدة على الشبكات المعرفة برمجياً من البيئات الحديثة التي تتطور يوماً بعد يوم ، لذا يعد أمن الشبكة مسألة هامة في هذا النوع من البيئات لنظراً للدور الهام الذي ستلعبه هذه الشبكات في منظومة النقل الذكي والمدن الذكية وما يرافق ذلك من تحديات أمنية معقدة، حيث تأتي أهمية البحث من خطورة هجمات حجب الخدمة الموزعة على المتحكمات في هذه الشبكات والخسائر التي يمكن أن تسببها للشركات والجهات التي تبدي اهتماما بتطبيق تقنية SD-VANET ، إضافة إلى أهمية تطبيق آلية أمنية فعالة تضمن زيادة مستوى الحماية للمتحكم في الشبكات في مواجهة هذه الهجمات.

وتبرز مبررات هذا الورقة في النقاط التالية:

أولا: يعتبر موضوع حماية المتحكمات من هجمات حجب الخدمة الموزع من المواضيع التي لايزال البحث فيها قائما، وبالتالي إمكانية التوصل الى نتائج مفيدة.

ثانيا: قلة الدراسات التي تعتمد على المعلومات الإحصائية التي توفرها لنا المتحكمات من الشبكة لكشف وصد هجمات منع الخدمة.

ثالثا: بعض الحلول تضيف عبء على أداء الشبكة من حيث التأخير والمعالجة وبعضها الآخر بحاجة الى إضافة تجهيزات على الشبكة.

طرائق البحث ومواده:

طُبّق سيناريو المحاكاة على برنامج (Mininet-WiFi)، الذي يعد أداة لمحاكاة سيناريوهات SDN / OpenFlow اللاسلكية التي تسمح بإجراء تجارب عالية الدقة تكرر بيئات الشبكات الحقيقية. يعزز Mininet-WiFi محاكي Mininet المعروف بمحطات لاسلكية افتراضية ونقاط وصول مع الحفاظ على إمكانات SDN الأصلية وبنية برامج المحاكاة الافتراضية مع دعم لبيئات شبكات VANET [6].

1. الدرسات المرجعية:

نظرا لأن هجوم DDoS هو أحد أكثر التهديدات شيوعا وخطورة للبنى القائمة على SDN، فقد ركزت معظم الدراسات في الأدبيات على مناهج التعلم الآلي لاكتشاف هذا الهجوم. استخدم الباحثون العديد من خوارزميات التعلم الآلي القائمة على التعلم الخاضع للإشراف وخوارزميات تصنيف التعلم العميق مثل K-Nearest Neighbors (KNN)، وآلة دعم المتجهات (SVM)، وشجرة القرار (DT)، و Naive Bayes (NB)، و Perceptron متعدد الطبقات (MLP)، والانحدار اللوجستي (LR)، والتمييز الخطي وغيرها.

يناقش المؤلفون في [7] طريقة لاكتشاف التهديدات في شبكات المركبات القائمة على SDN بناء على التعلم الآلي. يركز البحث بشكل خاص على الروابط بين السيارة والبنية التحتية (V2I). يحلل البيئة الحالية لإنشاء استراتيجية التعلم الآلي التي ستكتشف بنجاح التهديدات التي تشكلها هجمات حجب الخدمة الموزعة (DDoS) (فيضانات TCP، فيضانات UDP). لتحقيق ذلك، فإنه يجمع سبعة عناصر مختلفة من البيانات الفعلية من تدفقات TCP و UDP عندما يهاجمها DDoS وعندما لا تكون كذلك. يتم تعليم الشبكة من خلال استخدام العديد من خوارزميات التعلم المختلفة

الخاضعة للإشراف اعتمادا على البيانات المكتسبة، ويتم اكتشاف أن نهج SVM الخطي تنتج نتائج قريبة جدا من أن تكون الأفضل.

في [8]، قام المؤلفون بتحليل هجمات DDoS في شبكة المركبات القائمة على SDN من خلال استخدام فيضان TCP أو فيضان UDP أو فيضان ICMP. تم اعتماد مخططاً للكشف عن هجمات رفض الخدمة الموزعة (DDoS) في أجواء SDVN باستخدام ثلاثة نماذج منفصلة وهي. "نموذج الكشف عن المشغل" للحزم الواردة وطريقة أخرى هي "نموذج الكشف المستند إلى ميزة جدول التدفق". تستخدم كلتا الطريقتين ميزات بروتوكول OpenFlow واكتشاف نموذج تهديد يعتمد على تصنيف آلة متجه الدعم. يتم استخدام كل هذه النماذج جنبا إلى جنب مع بعضها البعض. قاموا بتجميع ومحاكاة حركة مرور الشبكة لاستيعاب هجمات DDoS المختلفة عبر Scapy و hping3 ، وأشارت النتائج إلى كفاءة تزيد عن 97٪.

في [9]، تم استخدام مصنفات مختلفة للتعلم الآلي للكشف عن هجمات DDoS التي تستهدف شبكات SD-VANET. أولاً، تم الحصول على مجموعة بيانات تحتوي على ميزات حركة مرور الشبكة العادية وحركة مرور شبكة هجوم DDoS من طوبولوجيا SD-VANET التي تم إنشاؤها تجريبيًا. تم استخدام خوارزمية اختيار ميزة الحد الأدنى من التكرار والحد الأقصى (MRMR) لتحديد الميزات الأكثر تميزًا في مجموعة البيانات. تم تدريب واختبار مصنفات التعلم الآلي باستخدام مجموعات البيانات الأصلية ومجموعات البيانات المطبقة الخاصة باختيار الميزات. توضح النتائج أن اختيار ميزة MRMR قد نجح في اكتشاف هجمات DDoS على SD-VANETs.

من الناحية العامة، هناك بعض النقاط التي يمكن أن تعتبر نقاط ضعف في هذه الدراسة:

- استخدمت الدراسة مجموعة بيانات تم إنشاؤها تجريبيًا لتمثيل حركة المرور في شبكات SD-VANET قد يكون هذا غير واقعي وقد يؤثر على قدرة النموذج على التعرف على الهجمات الحقيقية في الشبكات الحقيقية.
- استخدمت الدراسة خوارزمية Minimum Redundancy Maximum Relevance (MRMR) لتحديد الميزات الأكثر أهمية. قد يكون هناك خوارزميات أخرى تعطي نتائج أفضل أو تعالج تحديد الميزات بشكل أفضل.

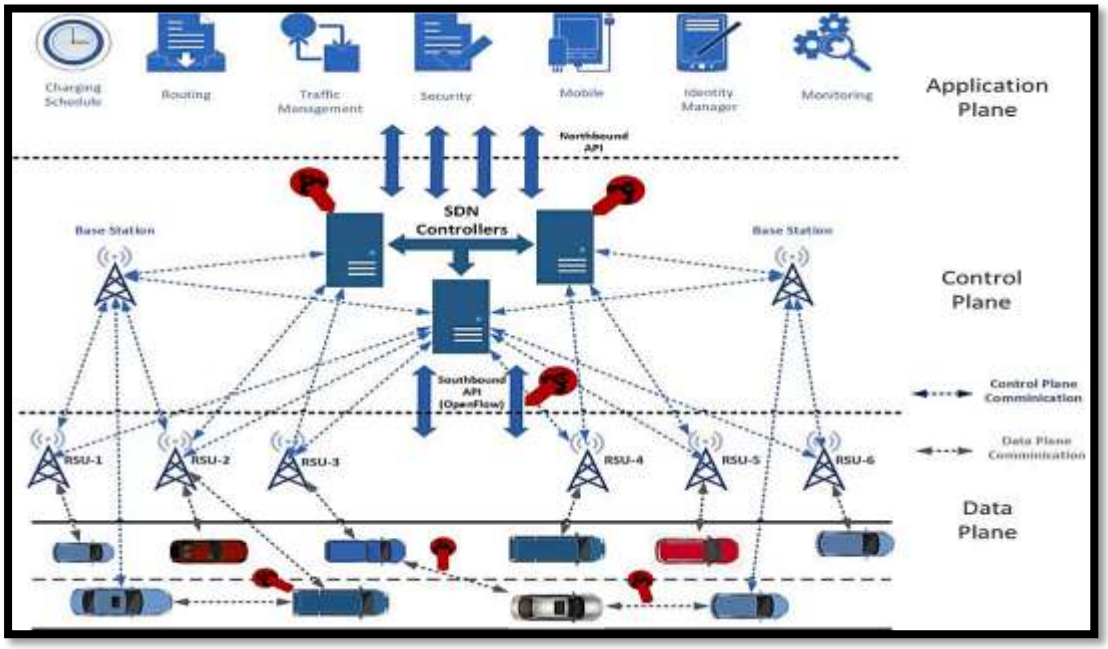
اقترحت [10] تقنية SVM متقدمة (ASVM)، وهي نسخة محسنة من SVM الحالية، للكشف عن هجمات DDoS في بنية SDN لتقليل أنشطة الدخيل. تقنية ASVM هي طريقة تصنيف تتكون من فئات متعددة. لقد استخدموا طريقة ASVM لتقصير أوقات التدريب والاختبار. وباستخدام التقنية التي استخدموها، حققوا دقة في الكشف عن الهجوم بنسبة 97%. ولكن كانت التجارب على شبكات SDN العادية.

استخدمت [11] نماذج التعلم الآلي DT وSVM وKNN وNB باستخدام ميزات قائمة على التدفق لاكتشاف هجمات DDoS على SDN. تم الحصول على أعلى دقة باستخدام نموذج DT بمعدل 95.16%. يعمل النموذج المقترح في الوقت الفعلي لاكتشاف الهجمات في SDN التقليدية. تتم مراقبة تدفق حركة مرور الشبكة بشكل مستمر من خلال نموذج التعلم الآلي القائم على التدفق لاكتشاف الهجمات. ولكن كانت التجارب على شبكات SDN العادية.

في [12] تم إنشاء بنية SDN على منصة محاكاة Mininet. تم تنفيذ هجمات DDoS في ثلاث فئات مختلفة (هجوم جدول التدفق، وهجوم عرض النطاق الترددي، وهجوم وحدة التحكم) باستخدام أداة Scapy على جدول تدفق أجهزة النقل التي كانت متوفرة في مستوى البيانات وعلى خط النقل الموجود بين وحدة التحكم. ومستوى البيانات. قاموا بتطبيق أربع خوارزميات للتعلم الآلي (SVM، MLP، DT وRF) للكشف عن هجمات DDoS. تم الحصول على أعلى دقة باستخدام خوارزمية التردد اللاسلكي. ولكن كانت التجارب على شبكات SDN السلكية العادية.

2. هجمات DDoS الخاصة ببنية SD-VANET:

في هجمات DDoS التي يتم إجراؤها ضد شبكات SD-VANET، يمكن اختيار مستوى التحكم ومستوى البيانات وخط الاتصال بين هاتين المستويتين كنقطة هدف للهجوم كما هو موضح في الشكل (2) [13,14].



الشكل (2) ببنية SD-VANET

1.2. هجمات DDoS تستهدف المتحكم:

أخطر هجمات DDoS على شبكات SD-VANET هي الهجمات ضد وحدة التحكم، والتي تعتبر عقل الشبكة الموجود في مستوى التحكم كما هو موضح في الشكل (2). حيث ترسل طلبات غير مرقمة إلى مبدلات sdn عن طريق المركبات. ومع زيادة طلبات قاعدة التدفق الجديدة، يتم تحميل قدرة المعالجة واتصال وحدة التحكم بشكل زائد. وبالتالي فإن الموارد المحدودة لوحدة التحكم مثل الحوسبة والذاكرة وعرض النطاق الترددي سوف تنفد بعد فترة. تصبح وحدة التحكم التي تنفد مواردها غير قادرة على الاستجابة لطلبات قاعدة التدفق الجديدة. وفي النهاية، ينقطع الاتصال بين مستويات SD-VANET بسبب انهيار وحدة التحكم. تتعطل بنية SD-VANET حتمًا. هذا النوع من الهجمات الذي قد يحدث ضد وحدة التحكم يمكن أن يتسبب في خسائر فادحة على الطريق وازدحام مروري كبير[15] وهي الهجمات التي ستركز عليها هذه الورقة البحثية.

2.2 هجمات DDoS تستهدف مستوى البيانات:

يتم توفير سلامة حركة البيانات بين المركبات ووحدة التحكم من خلال بروتوكول OpenFlow في SD-VANET يمكن لوحدة التحكم تعديل أو حذف أو إضافة إدخالات تدفق جديدة إلى جدول التدفق الموجود على وحدة RSU بواسطة بروتوكول التدفق إذا سيطر مهاجم على بروتوكول OpenFlow، فسيكون قادرًا على اعتراض تدفق البيانات بين وحدة التحكم والمركبات، والاستيلاء على مستوى البيانات بأكمله. علاوة على ذلك، عند الاستماع إلى هذا الخط، يمكن للمهاجم إضافة قواعد ضارة إلى قواعد الإرسال المرسلة من قبل وحدة التحكم ومنع الإرسال الصحيح لرزم البيانات.

3.2 هجمات DDoS ضد خط الاتصال بين المتحكم ومستوى طبقة البيانات:

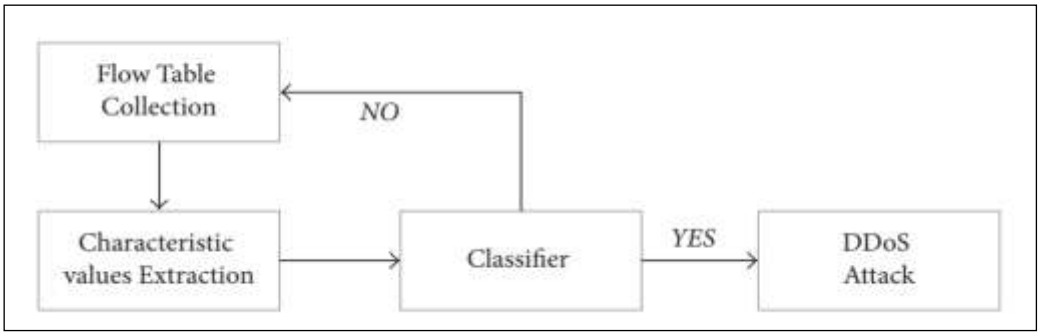
نظرًا لأن وحدة RSU لديها سعة تخزين محدودة، فمن المستحيل تخزين كافة القواعد التي تغطي كافة التدفقات. عندما تصل الرزم من عنوان غير معروف، يؤدي ذلك إلى إضافة القواعد الواردة حديثًا إلى جدول التدفق الخاص بوحدة RSU. عندما يرسل مهاجم حزمًا غير مرقمة من عنوان غير معروف خلال فترة قصيرة، تكتب وحدة التحكم قواعد لهذه الحزم وترسلها إلى جدول تدفق وحدة RSU. يتم ملء جدول التدفق ذو سعة التخزين الأقل في وقت قصير، ولا تبقى مساحة للقواعد الجديدة. ولذلك، يتوقف إرسال حركة المرور المسموح بها، باستثناء جدول التدفق، وتصبح ذاكرة التخزين المؤقت للتدفق أيضًا هدفًا لهجمات DDoS.

4. كشف الهجوم:

عادةً، تتكون حركة تدفق البيانات على الشبكة من مجموعة من حركة البيانات العادية والضارة. نحتاج إلى مراقبة وتحليل حركة المرور هذه لمنع انتهاك السياسات والحماية من الهجمات. لا يساعد حظر عنوان IP للمهاجمين المفترضين في تخفيف الهجوم بسبب انتحال عنوان IP؛ **وبالتالي، نحن بحاجة إلى التركيز على خصائص الهجوم حتى نتمكن من التخفيف منه.** من الصعب جدًا اكتشاف هجمات DDoS نظرًا لتشابهها مع حركة المرور العادية. ومع ذلك، هناك بعض الميزات المشتركة بين جميع هجمات DDoS. أولاً، الرزم الضارة المستخدمة في هجوم DDoS لها نفس عناوين الوجهة والمنفذ. تتمتع هذه الحزم أيضًا بحجم نموذجي يختلف عن حجم حركة المرور المشروعة. وتعد سرعة الكشف والدقة والموثوقية لنظام الكشف عن الهجوم أمر حيوي لضمان قيام الشبكة بوظائفها بشكل صحيح دون أي تأثير سلبي على المستخدمين. لذلك يمكن استخدام تقنيات التعلم الآلي لتحديد هجمات DDoS وحركة المرور العادية وبالتالي التخفيف من هجمات DDoS [16].

بعض الميزات التي يمكن أن تساعد في اكتشاف هجوم DDoS هي عدد الرزم، ومتوسط حجم الحزمة، وعدد البايتات، والرزم ومعدل البت، وما إلى ذلك. سيركز بحثنا على استخدام مصنف التعلم الآلي شائع الاستخدام للكشف عن الحالات الشاذة، مثل SVM.

يتطلب الكشف عن الهجوم بشكل أساسي توفر مجموعة حالة التدفق، وقيم خصائص الاستخراج، وحكم المصنف، كما هو موضح في الشكل (3). ترسل مجموعة حالة التدفق (Flow Status Collection) بشكل دوري طلب جدول تدفق إلى مبدل OpenFlow. بعدها يتم ارسال معلومات جدول التدفق التي تم الحصول عليها من المبدل إلى مجموعة حالة التدفق. تنتقل بعدها الى مستخرج القيم المميزة، وهو مسؤول بشكل أساسي عن استخراج القيم المميزة المتعلقة بهجوم DDoS من جدول التدفق وتكوين مصفوفة القيم المميزة المكونة من خمس مجموعات. يتم تصنيف معلومات القيم المميزة المكونة من خمس مجموعات باستخدام خوارزمية تستند إلى SVM للتمييز بين حركة تدفق البيانات العادية وحركة تدفق البيانات غير الطبيعية (المهاجمة).



الشكل (3) عملية الكشف عن الهجوم.

يتم جمع معلومات حالة جدول التدفق بشكل أساسي من خلال بروتوكول OpenFlow. يستجيب المبدل لرسالة op_flow_stats_request التي ترسلها وحدة التحكم بشكل دوري، ويجب أن يكون الفاصل الزمني بين الحصول على جداول التدفق معتدلا، مع ضبط فترة الحصول على جدول التدفق لتكون متسقة مع وقت حذف التدفق الذي حددته وحدة التحكم (Ryu controller) وتكون معلومات جدول التدفق المستخرجة بواسطة المبدل كما في الشكل (4).

الشكل (4) معلومات جدول التدفق المستخرجة

مبررات الطرح: تحافظ رزم هجوم DDoS على عدد منخفض نسبيًا من الاتصالات مع المبدل بسبب استخدام رزم IP المخادعة، كما تم العثور على عدد منخفض من الرزم المنقولة لكل اتصال مقارنة بالمستخدم الشرعي المتصل بالمبدل.

1.4. استخراج القيم المميزة.

عندما يحدث هجوم DDoS على الشبكة، سيتم بشكل عشوائي تزوير عدد كبير من عناوين IP المصدر لإرسال عدد معين من الرزم لمهاجمة الهدف. في الشبكة، يلاحظ أن تدفق الهجوم يُبدي تشابهاً وانتظاماً معيناً، ومن ثم يمكن اكتشافه من خلال تحليل معلومات القيم المميزة لجدول التدفق وهي على النحو التالي.

- تعداد عناوين IP المصدر (SSIP: Standard deviation of packets): هي عدد عناوين IP المصدر في كل وحدة زمنية:

SSIP=Sip/T

Sip: تعداد عناوين المصدر في جدول التدفق

T: فترة أخذ العينات

في حالة حدوث هجوم، يتم إنشاء عدد كبير من الهجمات عن طريق التزوير العشوائي لإرسال رزم البيانات، وسيزداد رقم عنوان IP المصدر بسرعة في جدول التدفق وهو معامل مهم من معاملات الكشف التي سنعتمدها.

- الانحراف المعياري لرزم التدفق (SDFP: Standard deviation of packets)، أي الانحراف المعياري لعدد الرزم في الفترة T، هو كما يلي:

SDFP = sqrt((1/n) * sum ((packets_i − mean_packets,2) 2))

packets_i عدد رزم التدفق في فترة أخذ العينات:

mean_packets: متوسط إجمالي الرزم لجميع التدفقات في فترة أخذ العينات

تشير n الى العدد الإجمالي لإدخالات التدفق لكل فترة، في حالة حدوث هجوم، تكون حجم رزم بيانات الهجوم العامة صغيرة نسبيا أما عددها يكون كبيراً. وسيكون الانحراف المعياري لرزم تدفق الهجوم أصغر من حالة التدفق العادي.

- انحراف بايت التدفق (SDFB: Deviation of Flow Bytes)، أي الانحراف المعياري لعدد البايتات في الفترة T:

$$SDFB = sqrt((1/n) * sum ((bytes\_i - mean\_bytes,2)^2))$$

bytes_i عدد إجمالي بايتات التدفق في فترة أخذ العينات:

mean_bytes: متوسط إجمالي البايتات لجميع التدفقات في فترة اخذ العينات

في حالة حدوث هجوم، ومن أجل تقليل تحميل الرزم، سيرسل المهاجم أجزاء أصغر من رزم البيانات وستكون الانحراف المعياري لبتات التدفق أصغر من التدفق العادي.

- تعداد إدخالات التدفق (SFE: speed of flow entries)، أي عدد إدخالات التدفق لكل وحدة زمنية SFE=N/T

في حالة حدوث هجوم، يزداد عدد إدخالات التدفق لكل وحدة زمنية بشكل كبير، وهو أعلى بكثير من القيمة العادية.

- نسبة التدفق الزوجي (RPF: Ratio of Pair-Flow)، أي نسبة إدخالات التدفق التفاعلي إلى إجمالي إدخالات التدفق، هي كما يلي:

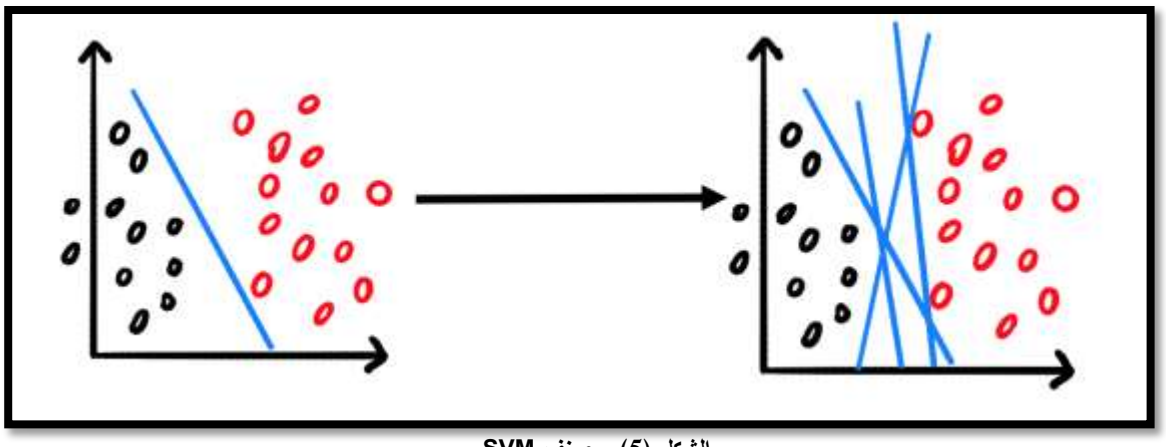
$$RPF= 2* pair\_sum/N$$

حيث pair_sum هو عدد إدخالات التدفق التفاعلي. في ظل الظروف العادية، يرسل المضيف المصدر طلبا إلى المضيف الوجهة لإنشاء تدفق تفاعلي.

الخلاصة: عند حدوث هجوم، فإن إدخالات التدفق المرسلة باتجاه المضيف الوجهة في فترة T تزيد بشكل حاد، ولا يمكن للمضيف الوجهة الاستجابة للتدفق التفاعلي في الوقت المناسب، وبشكل عام يستخدم المهاجم عادةً عناوين مصدر زائفة ضخمة عند الهجوم، وبالتالي فإن عدد مدخلات التدفقات التفاعلية ستنخفض في الفترة T.

بالتالي سيتمكن المتحكم عن طريق مقارنة تغيرات قيم المعاملات السابقة من تحديد الهجوم وكشفة.

يعد SVM خوارزمية تصنيف، وهي تستخدم بشكل أساسي للتصنيف الثنائي. يتم عادةً فصل البيانات إلى فئتين من نقاط البيانات ثم يتم النظر فيها هندسيًا للعثور على المصنف. ويبين الشكل (5) مثالاً بسيطًا لإيجاد التصنيف. حيث أن فئتا البيانات عبارة عن نقاط سوداء وحمراء والخط الأزرق هو المصنف.



الشكل (5). مصنف SVM

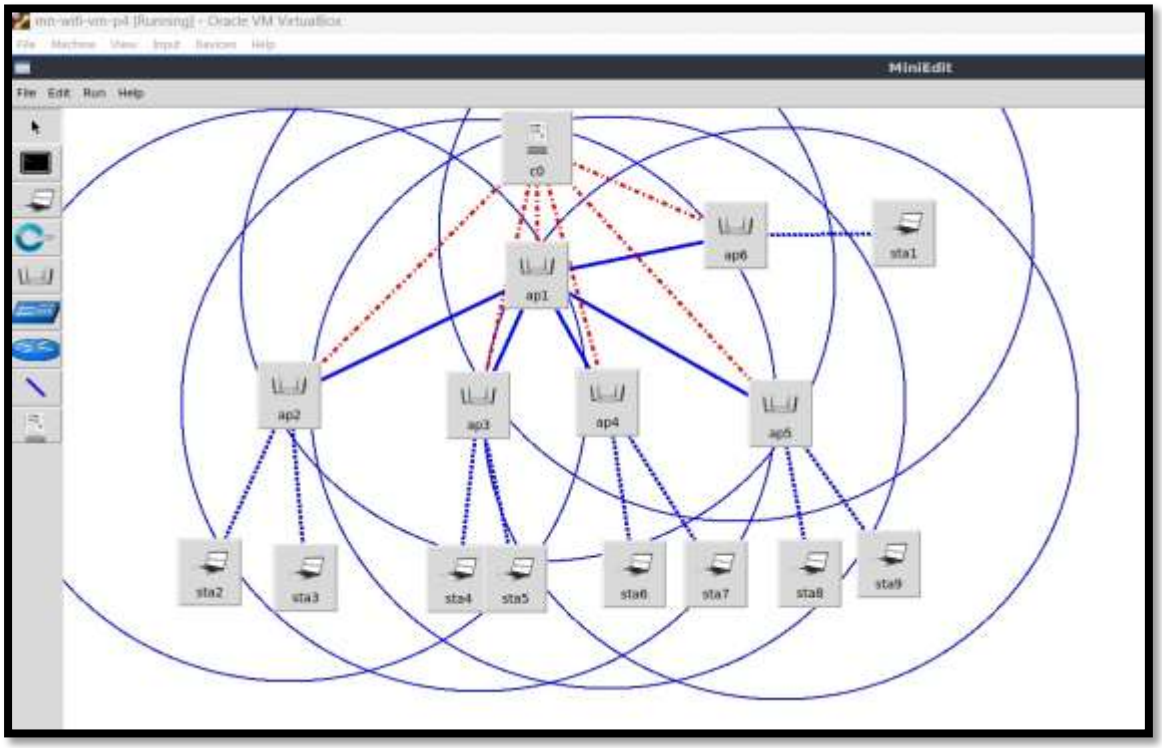
وتعد خوارزمية التصنيف SVM ذات مردود جيد جداً لمهام التصنيف[17,18] . حيث يتم تصور نقاط البيانات المختلفة ويقوم حد القرار أو المستوى بفصل فئة نقاط البيانات عن بعضها. يمكن أن يكون حد القرار خطًا مستقيمًا أو مستوي، ويعتمد ذلك على عدد نقاط البيانات. تُعرف النقاط الأقرب إلى مستوى القرار باسم المتجهات الداعمة التي

تساعد في حساب هامش مستوى القرار. يعد مستوى القرار بهامش كبير أفضل من الهامش الصغير. إن مستوى القرار الأمثل هو مستوى قرار معمم ويفصل بشكل أفضل بين الفئات المختلفة. بالتالي سيتم استخدامه في هذا البحث لأنه يعمل بشكل جيد من أجل التصنيف مع عدد محدد أو قليل من الميزات كما في حالتنا.

5. تصميم وتنفيذ التجربة.

تتضمن خطوات عملية الدراسة مراحل الحصول على مجموعة البيانات، واختيار الميزات، وتطبيع البيانات، وتقسيم مجموعة البيانات، والتدريب، والاختبار على النحو التالي:

إنشاء مجموعة البيانات: الخطوة الأولى هي جمع البيانات الأولية. لذلك تم إنشاء طوبولوجيا SD-VANET تجريبية للحصول على مجموعة بيانات تحتوي على هجمات DDoS وبيانات حركة مرور الشبكة العادية. تمت محاكاة سيناريو الشبكة في منطقة تبلغ مساحتها 1000 م × 500 م. باستخدام MINIEDIT ضمن MININET-WIFI وبعد ذلك تمت عمليات المحاكاة. يظهر الشكل (6) طوبولوجيا الشبكة المستخدمة. وتتكون الطوبولوجيا من ست وحدات(ap) RSU، 9 مركبات (sta 1..... sta 9) ، ووحدة تحكم أساسية واحدة RUY.



الشكل (6) طوبولوجيا الشبكة المستخدمة

في السيناريو المعتمد ستكون العقدة sta1 الهدف الضحية المتصلة مع ap6. يمكن لـ sta2 إرسال رزم عادية لإنشاء عينات عادية ثم بعد ذلك تقوم نفس العربة بإرسال رزم هجوم DDoS لإنشاء عينات هجوم DDoS. يقوم sta3 sta9 بإنشاء عينات حركة مرور الشبكة العادية. سيتم استخدام هذه العينات للتدريب على إنشاء نموذج جديد لاكتشاف الهجوم.

ستكون أداة هجوم DDoS الكلاسيكية Hping3 هي المستخدمة لإنشاء حركة مرور غير طبيعية للشبكة. Hping3 قابل للبرمجة النصية بالكامل، وتستخدم لإنشاء أنواع مختلفة من بيانات الهجوم [17,18].

في هذه الدراسة سيتم إنشاء هجمات DDoS من نمط هجمات رسائل (ICMP). تم إجراء محاكاة تجريبية لجمع كل من بيانات هجمات DDoS وبيانات حركة مرور الشبكة المنتظمة الطبيعية. أثناء المحاكاة، تم إرسال حزمICMP في البداية كرزم عادية، ثم كرزم هجوم DDoS بعد ذلك. تتكون مجموعة البيانات من 4000 عينة، تحوي كل عينة على البارامترات الخمس التي تقيم حركية الشبكة بالإضافة الى نوع هذه الحركية (طبيعية أو هجوم) كما هو موضح في الجدول (1):

الجدول (1): بارامترات تقييم حركية الشبكة مع تحديد نوع الحركية (طبيعية أو هجوم) 4000 rows × 6 columns

	SSIP	Stdevpack	Stdevbyte	NbFlow	NbIntFlow	Class
0	41	0.389776	75.804607	41	0.516129	1
1	41	0.450748	119.721586	41	0.516129	1
2	13	0.835165	351.018887	26	1.000000	0
3	13	0.714143	307.680791	26	1.000000	0
4	11	0.588235	334.996292	22	1.000000	0
...	...	...	...	...	...	...
3995	12	0.721688	333.682848	24	1.000000	0
3996	12	0.821678	313.412966	24	1.000000	0
3997	41	0.279828	85.944815	41	0.516129	1
3998	41	0.279828	84.437979	41	0.516129	1
3999	12	0.670407	330.257404	25	1.000000	0

يتم بعد ذلك تحديد بيانات مصنف التعلم الآلي باستخدام المعلمات الخمسة المختارة سابقاً، ثم تقسيم مجموعة البيانات إلى عينات تدريب بنسبة 80% وعينات اختبار بنسبة 20%. لضمان دقة وفعالية عملية التدريب، تم تقييس القيم الموجودة في قاعدة البيانات لتتراوح بين 0 و1 باستخدام أداة التقييس Standard Scaler بعد ذلك، تم تدريب نموذج SVM باستخدام نواة خطية (linear kernel) على بيانات التدريب.

النتائج والمناقشة:

1. مصفوفة الارتباك

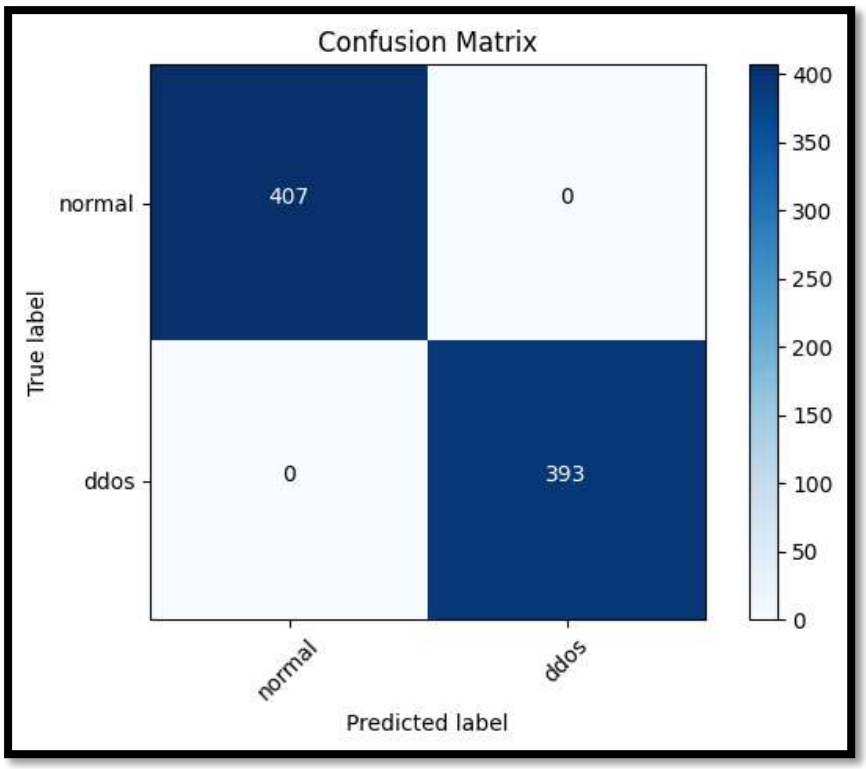
مصفوفة الارتباك الموضحة في الشكل (7) تعتبر أداة فعالة لتقييم أداء نموذج التعلم الآلي المستخدم في الكشف عن هجمات حجب الخدمة الموزعة (DDoS) ضمن شبكات SD-VANET تتكون المصفوفة من أربع مربعات تمثل العلاقة بين التنبؤات التي قام بها النموذج والنتائج الفعلية في مجموعة البيانات المستخدمة.

المحور العمودي (True label) يمثل الفئات الفعلية للعينات في مجموعة الاختبار. في هذه الحالة، لدينا فئتين "normal"(أي حركة مرور عادية) و "ddos" أي هجماتDDoS .

المحور الأفقي (Predicted label) يمثل الفئات التي تم التنبؤ بها من قبل النموذج.

- **العناصر داخل المصفوفة:**
- **True Positives (TP)**الرقم 393 في المربع السفلي الأيمن يمثل عدد العينات التي كانت فعلاً هجمات DDoSوتعرف عليها النموذج بشكل صحيح.
- **True Negatives (TN)**الرقم 407 في المربع العلوي الأيسر يمثل عدد العينات التي كانت فعلاً غير هجمات DDoS وتعرف عليها النموذج بشكل صحيح.
- **False Positives (FP)**الرقم 0 في المربع العلوي الأيمن يمثل عدد العينات التي كانت غير هجمات DDoSلكن النموذج تعرف عليها خطأً على أنها هجمات. في هذه الحالة، لا يوجد أي خطأ من هذا النوع.
- **False Negatives (FN)**الرقم 0 في المربع السفلي الأيسر يمثل عدد العينات التي كانت هجمات DDoSولكن النموذج لم يتعرف عليها، وتم تصنيفها خطأً على أنها حركة مرور عادية. أيضًا، لا يوجد أي خطأ من هذا النوع.

بما أن المصفوفة لا تحتوي على أي قيم لـ False Positives أو False Negatives ، فإن دقة النموذج تصل إلى 100%. هذا يعني أن النموذج كان قادراً على تصنيف جميع العينات بشكل صحيح دون أي أخطاء.



الشكل (7): مصفوفة الارتباك

2. تقرير المصنف

	precision	recall	f1-score	support
0	1.00	1.00	1.00	407
1	1.00	1.00	1.00	393
accuracy			1.00	800

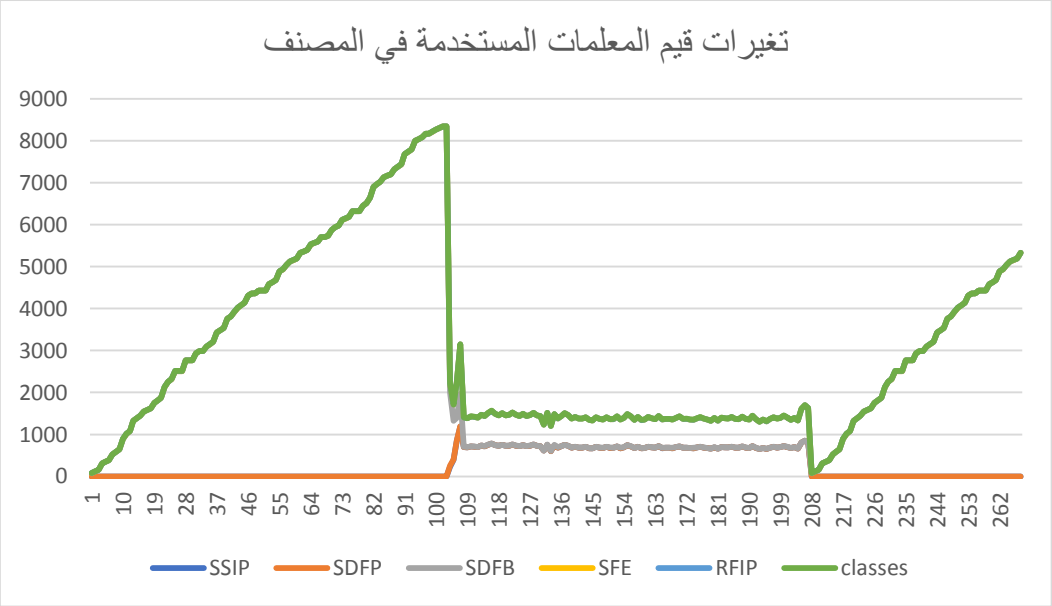
macro avg	1.00	1.00	1.00	800
weighted avg	1.00	1.00	1.00	800

نلاحظ أن F1–Score (مقياس F1) وهو المتوسط التوافقي للدقة والاستدعاء، ويعطي فكرة عن توازن الأداء بين الدقة والاستدعاء. في هذا التقرير، مقياس F1 لكل من الفئتين 0 و 1 هو 1.00، مما يشير إلى أداء مثالي. وأن الدقة العامة هي 1.00، مما يعني أن النموذج صنف جميع العينات بشكل صحيح.

بشكل عام، هذا التقرير يشير إلى أن النموذج يعمل بشكل مثالي على مجموعة البيانات هذه، حيث حقق دقة واستدعاء ومقياس F1 بنسبة 100% في جميع الفئات.

يوضح الشكل (8) التغير الواضح على قيم المعاملات الأساسية التي يستخدمها المصف لاكتشاف وتحديد الهجوم. نلاحظ التغيرات الواضحة عند النافذة 101. مع العلم أن تدفق البيانات على الشبكة طبيعي من 0 حتى 101 ومن 208 حتى نهاية المحاكاة.

التغيرات الواضحة في قيم هذه المعاملات بين الحالة الطبيعية وحالة الهجوم تؤكد وتثبت صوابيه اعتماد هذه المعاملات في تحديد الهجوم وكشفة. وهذا ما أكدته النتائج التي تم الحصول عليها.



الشكل (8) تغيرات قيم المعاملات الأساسية التي يستخدمها المصف لاكتشاف وتحديد الهجوم

الاستنتاجات والتوصيات:

في هذه الورقة، تم جمع معلومات حالة التدفق لحركة مرور الشبكة بواسطة وحدة التحكم. وتم استخراج القيم المميزة المكونة من خمس ميزات والمتعلقة بهجوم DDoS ثم استخدمنا خوارزمية المصنف SVM للحكم على حركة المرور وتنفيذ اكتشاف هجوم DDoS.

تم التركز على تحليل التغيرات في القيم المميزة لحركة تدفق البيانات والتحقق من جدوى هذه الطريقة من خلال النتائج. وكانت البنية المنفذة قادرة على تلبية جميع المتطلبات المطروحة خلال مرحلة التحليل. في الواقع، يتمكن النظام من اكتشاف الهجوم في وقت قصير، وبالتالي الحد من الضرر الذي يلحق بالشبكة ووحدة التحكم.

كعمل مستقبلي يمكن العمل على نهج يتمثل في إنشاء خادم تحليل منفصل للبحث والتطوير في الشبكة المقترحة. يتمتع هذا الخادم بذاكرة وموارد معالجة كبيرة وكافية. عندما يُتوقع أن تكون رزم المضيف عبارة عن هجوم DDoS، يتم إرسال أمر لإنشاء إدخال تدفق من منفذ المهاجم إلى خادم التحليل من خلال وحدة التحكم. سيتم إرسال جميع الرزم الجديدة من عقدة الهجوم إلى خادم التحليل لفترة. يقوم خادم التحليل المجهز بقدرات التحليل والمراقبة القوية بفحص الرزم الملتقطة لتحسين اكتشاف وفعالية العملية بأكملها.

References:

[1] A. Tesfanesh, “Software-Defined Networking (SDN) based VANE Architecture: Mitigation of Traffic Congestion”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 3, 2020.

[2] Z. Li, K. Wang, T. Yu and K. Sakaguchi, "Het-SDVN: SDN-Based Radio Resource Management of Heterogeneous V2X for Cooperative Perception," in IEEE Access, vol. 11, pp. 76255-76268, 2023.

[3] D. Venkatramana, S. Srikantaiah, & J. Moodabidri, "Scgrp: sdn-enabled connectivity-aware geographical routing protocol of vanets for urban environment”, IET Networks, vol. 6, no. 5, p. 102-111, 2017.

[4] M.Uddin, K. Mohammad, and A. Jahanara.” Implementing AODV Routing Protocol in VANET using SDN”. International Journal of Computer Applications. Vol. 175 – No. 32, November 2020.

[5] . H. Hussein et al., "SDN-Based VANET Routing: A Comprehensive Survey on Architectures, Protocols, Analysis, and Future Challenges," in IEEE Access.2024.

[6] https://github.com/intrig-unicamp/mininet-wifi/issues, 2024.

[7] P. K. Singh, S. Kumar Jha, S. K. Nandi and S. Nandi, "ML-Based Approach to Detect DDoS Attack in V2I Communication Under SDN Architecture," TENCON 2018 - 2018 IEEE Region 10 Conference, Jeju, Korea (South), pp. 0144-0149,2018.

[8] Yu Y, Guo L, Liu Y, et al, “An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks”. IEEE Access 6:44570–44579,2018.

[9] M. Turkoglu, H. Polat,” Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection”, Expert Systems with Applications, Vol .203,2022.

[10] O. Myint,S. Kamolphiwong, , “Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN)”. Journal of Computer Networks and Communications, 2019.

[11] N. Satheesh, , M. Rathnamma, “Flow-based anomaly intrusion detection using machine learning model with software defined networking for OpenFlow network”. Microprocessors and Microsystems, 79, Article 103285. 2020.

[12] R. Santos, D. Souza,” Machine learning algorithms to detect DDoS attacks in SDN”. Concurrency Computation, 32(16), 1–14.2020.

[13] R. Ujjan, Z. Dahal, "Towards s Flow and adaptive polling sampling for deep learning-based DDoS detection in SDN". Future Generation Computer Systems, 111, 763–779. 2020.

[14] M. Türkoğlu, H. Polat, Cocoa, O. Polat, "Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection", Expert Systems with Applications, Vol. 203,2022.

[15] M. Ali Setitra and M. Fan., "Detection of DDoS attacks in SDN-based VANET using optimized TabNet". Comput. Stand. Interfaces 90, Aug 2024.

[16] B. Liu, D.Tang, J. Chen, Wei Liang, Y. Liu, Q.Yang,"ERT-EDR: Online defense framework for TCP-targeted LDoS attacks in SDN",Expert Systems with Applications, Vol. 254,2024.

[17] H. Alqahtani and M. Abdullah, "A Review on DDoS Attacks Classifying and Detection by ML/DL Models" International Journal of Advanced Computer Science and Applications (IJACSA), 15(2), 2024.

[18] K. Alhamami and S. Albermany, "DDOS attack detection using machine learning algorithm in SDN network," 2023 Al-Sadiq International Conference on Communication and Information Technology (AICCIT), Al-Muthana, Iraq, pp. 97-102, 2023.