Using Machine Learning Algorithms for Cybersecurity in CAVs

Dr. Ali Esmaeel*

(Received 11 / 2 / 2023. Accepted 5 / 7 / 2023)

□ ABSTRACT □

The digital world is vulnerable to security threats, and cyber security helps mitigate these threats. Cyber security refers to the protection of data, networks, systems, applications and all types of data from cyber attacks which include viruses and various types of attacks. Autonomous and Connected Vehicle Networks (CAVs) are widely used, and because of their wireless and self-driving properties; They are highly vulnerable to previous threats.

This research studies the techniques of using artificial intelligence to protect networks of CAVs from cyberattacks. It uses machine learning algorithms to detect these attacks and compares the machine learning algorithms used for this in terms of accuracy and required operating time. The research uses the WEKA tool to make the comparison, as the experiments are carried out on a a new dataset, which is a dataset abbreviated from the KDD99 dataset.

Two machine learning algorithms, Decision Tree and Naive Bayes, were used as classification models, based on a modified training dataset of the KDD99 dataset to be suitable for CAVs. The accuracy and runtime of these two models are compared and analyzed when selecting each type of communication-based attack. The obtained results show that the decision tree model requires a shorter runtime, which is more suitable for detecting a CAV communication attack.

Keywords: Connected and Autonomous Vehicle; cyber security; machine learning, Cyber attacks.

* **Assistant Professor, Department of Systems and Computer Networks, Faculty of Information Engineering, Tishreen University, Lattakia, Syria. AliEsmaiel@gmail.com**

استخدام خوارزميات تعلّم الآلة في تحقيق الأمن السيبراني في شبكات الآليات الذاتيّة والمتّصلة (CAVs)

د. علي اسماعيل*

(تاريخ الإيداع 11 / 2 / 2023. قُبِل للنشر في 5/ 7 / 2023)

□ ملخّص □

يُعدّ العالم الرقمي معرّضاً للتهديدات الأمنية، إذ يساعد الأمن السيبراني على التخفيف من هذه التهديدات. يشير الأمن السيبراني إلى حماية البيانات والشبكات والأنظمة والتطبيقات وجميع أنواع البيانات من الهجمات السيبرانية التي تشمل الفيروسات وأنواعاً مختلفة من الهجمات. تُستخدم شبكات الآليات الذاتية والمتّصلة (CAVs) على نطاق واسع، وبسبب خصائصها المتمثّلة بالاتصال اللاسلكي وذاتيّة القيادة؛ فإنّها تكون معرّضة للتهديدات السابقة بشكل كبير.

يدرس هذا البحث تقنيات استخدام الذكاء الاصطناعي لحماية شبكات CAVs من الهجمات السيبرانية. إذ يستخدم خوارزميات تعلّم الآلة للكشف عن هذه الهجمات ويقارن بين خوارزميات تعلّم الآلة المستخدمة لذلك من حيث الدقّة وزمن التشغيل اللازم. يستخدم البحث الأداة WEKA في إجراء المقارنة، إذ تنّفذ التجارب على مجموعة بيانات (dataset) جديدة مختزلة عن مجموعة البيانات KDD99.

استُخدمت خوارزميتان للتعلم الآلي، وهما Decision Tree و Naive Bayes كنموذجين للتصنيف. استناداً إلى مجموعة بيانات تدريب مُعدّلة عن مجموعة البيانات KDD99 لتصبح مناسبة لشبكات CAVs، يتم مقارنة وتحليل دقة ووقت تشغيل هذين النموذجين عند اختيار نوع من أنواع الهجمات القائمة على الاتصالات. بينت النتائج التي تمّ التوصّل إليها أنّ نموذج شجرة القرار يتطلّب وقت تشغيل أقصر، وهو أكثر ملاءمة لاكتشاف هجوم اتصالات CAVs.

الكلمات المفتاحية: الآليات الذاتية والمتصلة؛ الأمن السيبراني؛ تعلّم الآلة؛ الهجمات السيبرانية.

* **مدرّس- قسم النظم والشبكات الحاسوبية- كلية الهندسة المعلوماتية - جامعة تشرين- اللاذقية – سورية.**
AliEsmaiel@gmail.com

مقدّمة:

حوّلت التحسينات الرقمية عالمنا إلى مجتمع رقمي، والذي يكون معرّضاً لأنواع مختلفة من الهجمات. يعرّف الأمن السيبراني على أنّه حماية الأنظمة، الشبكات، التطبيقات، البيانات، وجميع أنواع البيانات من الهجمات السيبرانية. يعدّ الأمن السيبراني ضروري في العالم الرقمي. وهو مطلوب في النشاطات اليومية مثل التسوّق، الأعمال التجارية، والمناقلات، وجميع المهام المنجزة والمخزّنة على الأجهزة الحاسوبية.

يركّز البحث على الآلات الذاتيّة والمتّصلة (CAVs) التي كانت محطّ اهتمام وتركيز الكثير من البحوث والدراسات [1] [2]. تتميّز هذه الشبكات بمزايا الاتصال اللاسلكي وذاتيّة القيادة. يقصد بأنّها متّصلة "connected" أن الآليات تعتمد على البيانات المرسلة من الآليات الأخرى لتحدّد توجيه بياناتها واتصالاتها ضمن الشبكة المرتبطة. بينما يشير مصطلح الذاتية (autonomous) الكاملة إلى أنه بإمكانها قيادة المهام بشكل ديناميكي وتستعيد الأحداث بشكل أتوماتيكي في العالم الحقيقي بدون تدخّل من قائد (driver) [17].

بسبب خصائصها السابقة، تتعرّض شبكات CAVs إلى هجمات سيبرانية أكثر، وتكون معرّضة لتبادل البيانات مع البيئة الخارجية ومع الآليات الأخرى عبر مسارها [18]. توضّح الفقرات التالية نماذج الهجمات السيبرانية وكيفية استخدام الذكاء الاصطناعي في الحماية من هذه الهجمات.

1-1- نماذج الهجمات السيبرانية

تتراوح الهجمات من تثبيت برامج التجسس على جهاز حاسوب شخصي ويمكن أن تنتهي بمحاولة تدمير البنية التحتية لدول بأكملها. يمكننا توضيح بعض الهجمات على النحو التالي:

أ. فيروسات الحاسوب: هو برنامج ذاتي النسخ يمكنه ربط نفسه ببرنامج آخر لإعادة إنتاجه، لذلك من الصعب للغاية تعقبه لأنه يمكنه تغيير مواقعه الرقمية في أي وقت.

ب. Adware: هو برنامج ضارّ معروف بإنتاج رسائل منبثقة. ينشئ المتسلّلون برنامجاً جذّاباً، وعندما يقوم المستخدم بتشغيله، يمكنهم الدخول إلى حاسوب المستخدم وحذف بياناته أو استخدامها.

ج. حصان طروادة: هو نوع من البرامج الضارّة يقدّم نفسه كبرنامج مفيد ويتحكّم في الأنظمة. يمكنه تثبيت الفيروس في النظام، لكنّه لا يمكنه إعادة إنتاج نفسه. يمكنه حذف الملفات والبيانات المهمّة من حاسوب المستخدم وإرسال المعلومات إلى نظام المتسلّل.

د. فيروسات الفدية: هو فيروس يهاجم حاسوب المستخدم وابتزازه لكسب المال.

هـ. رسائل البريد الإلكتروني المخادعة: تُستخدم لسرقة المعلومات الشخصية للمستخدم. تُرسل رسائل البريد الإلكتروني الاحتيالية إلى المستخدم، ويتم التلاعب بها كما لو كانت من المسؤولين. يمنح هذا الفيروس المتسللين معلومات حول تفاصيل تسجيل الدخول لحسابات وسائل التواصل الاجتماعي المختلفة ومعلومات بطاقة الائتمان الأخرى.

تعدّ هجمات الرجل في الوسط (MITM) ورفض الخدمة (DoS) وحقن SQL و Botnets أنواعاً أخرى من التهديدات السيبرانية.

تتمثّل الوظيفة الرئيسية لخبراء الإنترنت في:

- البحث عن نقاط الضعف واختبارها وإصلاحها داخل البنية التحتية للشركة
- أنظمة مراقبة المحتوى الضار
- تحديد خروقات الشبكة

• تثبيت تحديثات البرامج والجدران النارية والحماية من الفيروسات بشكل منتظم
• تعزيز المناطق التي قد تكون قد وقعت فيها الهجمات

يستخدمون أساليب مختلفة للدفاع عن الأنظمة والشبكات من الهجمات. تتضمن بعض أفضل الممارسات ما يلي:

• استخدام المصادقة ثنائية الاتجاه
• تثبيت تحديثات منتظمة
• استخدام جدران الحماية لتعطيل الخدمات غير المرغوب بها
• توظيف التشفير أو التشفير
• تأمين مخدّمات اسم المجال DNS
• تجنّب حيل الخداع
• تشغيل برامج مكافحة الفيروسات
• تأمين كلمات المرور

يلعب نظام الأمن السيبراني دوراً حيوياً في الحفاظ على السلام والنظام في هذا العالم الرقمي الديناميكي.

1-2- الذكاء الاصطناعي في مجال الهجمات السيبرانية

طُوّرت العديد من تقنيات وأساليب الذكاء الاصطناعي مع مرور الوقت لمواجهة الهجمات السيبرانية. تُقسم هذه الأساليب إلى: الشبكة العصبية الاصطناعية (ANN)، والنظام الخبير، والوكيل الذكي، ولغة الآلة.

يتراوح الأمان في الذكاء الاصطناعي من استخدام برامج مكافحة الفيروسات/البرامج الضارة، ومنع فقدان البيانات، والكشف عن الاحتيال/مكافحة الاحتيال، وإدارة الهوية والوصول، ونظام كشف/منع التطفّل، وإدارة المخاطر. تهتّم الشركات الكبرى مثل Google وMeta وMicrosoft وAmazon وSpaceX وغيرها بامتلاك ملفّات تهديدات مجرمي الإنترنت. وفقًا لفينش: "يمكن استخدام الذكاء الاصطناعي لتحديد الأنماط في أنظمة الحاسوب التي تكشف عن نقاط الضعف في البرامج أو برامج الأمان، ممّا يسمح للمهاجمين باستغلال نقاط الضعف المكتشفة حديثاً". وبالتالي، إذا كان بإمكان خبراء الإنترنت التفكير في خطوة أبعد من تفكير هؤلاء المجرمين، فإنّ الذكاء الاصطناعي وحده سوف يعزّز الأمن السيبراني. خلافاً لذلك، سيحكم هؤلاء المهاجمون العالم. تشرح الفقرات التالية أساليب الذكاء الاصطناعي المستخدمة لمواجهة الهجمات.

1-2-1-الشبكة العصبية الاصطناعية (ANN): هي نموذج تعليمي إحصائي يحاكي السلوك البنيوي والوظيفي للدماغ البشري، أُنشئ لأول مرة كمفهوم في عام 1957 بواسطة فرانك روزنبلات. لدى ANN القدرة على التعلّم وحلّ المشكلات في المجالات المعقّدة المختلفة. في الأمن السيبراني، استخدمت الشبكات العصبية الاصطناعية في جميع المراحل الأربع لنهج الأمان المتكامل (تصنيف شامل لإطار الدفاع السيبراني)، ويتألف من مرحلة الإنذار المبكر، ومرحلة الوقاية، ومرحلة الاكتشاف، ومرحلة ردّ الفعل/الاستجابة. ينطبق تجنّب تقنيات كشف التسلّل أيضاً على الشبكات العصبية. بُنيت هذه الخطط في اكتشاف هجوم DoS ، وفلترة البريد العشوائي، وتحليل البرامج الضارّة، وعلوم الطب الشرعي.

1-2-2- النظام الخبير: تعدّ البرامج التخصصيّة أكثر أساليب الذكاء الاصطناعي شيوعاً. يمثّل برنامج الخبير تقنية للبحث عن حلول للمشكلات التي يسببها العميل أو تقنية معينة في مجال تكنولوجيا معين. يمكن استخدامها على وجه

التحديد في المساعدة على اتخاذ القرار، على سبيل المثال، في مجال الرعاية الطبيّة أو المصرفيّة أو العوالم الافتراضية.

هناك العديد من تقنيات التحسين لحلّ المشكلات المعقّدة من التشخيصات الطبيّة التحليلية الدقيقة إلى الأنظمة الهجينة المتقدّمة للغاية. يشتمل مخطّط الخبرة على قاعدة معرفيّة تحتوي على تحليل متخصّص لمجال تطبيق معين. للإشارة إلى قاعدة المعرفة، يحتوي هذا على محرّك يقدّم حلولاً تستند إلى هذا الفهم.

وفقًا لطريقة التفكير، يمكن للأنظمة الخبيرة حل نوعين من المشكلات:

• الاستدلال على أساس الحالة: يستدعي هذا النوع حالات المشكلة المماثلة السابقة، ويفترض أنّ الحلول لحالة المشكلة السابقة يمكن استخدامها لحلّ مشكلة جديدة. بعد ذلك، سوف يُقيّم الحلّ الجديد وقد يُراجع حسب الحاجة ثم يضاف إلى قاعدة المعرفة. يساعد هذا النهج باستمرار على تحسين دقّة النظام ويتعلّم المشكلات الجديدة تدريجياً.

• الاستدلال المستند إلى القواعد: يستخدم هذا النوع القواعد التي يحدّدها الخبراء لحلّ المشكلات. تتكون القواعد من جزأين: شرط وإجراء. تُحلّل المشكلات في خطوتين: أولاً، تُقيّم الحالة ثم يُتخذ الإجراء المناسب. على عكس الأنظمة المستندة إلى الحالة، لا يمكن للأنظمة المستندة إلى القواعد تعلّم قواعد جديدة أو تعديل القواعد الحالية تلقائياً.

1-2-3- الوكيل الذكي: الوكيل الذكي (IA) هو كيان خاضع للرقابة الذاتية مع آلية صنع قرار داخلية منفصلة وهدف شخصي. إنه يراقب من خلال أجهزة الاستشعار ويراقب المجال باستخدام المشغلات ويتحكم في إجراءاته نحو تحقيق الأهداف. يمكن أن يتعلّم العملاء الأذكياء المعلومات أو يستخدمونها لتحقيق أهدافهم. قد يكون لديهم أيضاً خصائص سريعة الاستجابة، وعند التواصل مع وكلاء مستقلين آخرين قد يفهمون ويستجيبون للتغييرات في مجالهم. هذا يمكنهم من اكتساب الخبرة بمرور الوقت من خلال التعلم والتواصل مع بيئتهم. استُخدم IA لتجنّب هجمات رفض الخدمة الموزعة (DDoS).

1-2-4 لغة الآلة: توفّر ML للأنظمة القدرة على اكتشاف وإضفاء الطابع الرسمي على المبادئ التي تقوم عليها تلك البيانات، والتعلّم من خلال البيانات، والتحسين من التجربة دون أن تُبرمج بشكل صريح. تبدأ عملية التعلم بمراقبة البيانات من خلال الأمثلة للبحث عن أنماط في البيانات واتخاذ قرار أفضل في المستقبل بناءً على الأمثلة المعطاة. مع هذه المعرفة، يمكن للخوارزمية أن تفكّر في خصائص الأمثلة غير المرئية سابقاً. يستخدم ML الإحصائيات لاستخراج المعلومات واكتشاف الأنماط واستخلاص النتائج حتى أثناء استخدام كمية هائلة من البيانات. هناك أنواع مختلفة من خوارزميات تعلّم الآلة. يمكن أيضاً تصنيفها في ثلاث فئات رئيسية:

• التعلّم الخاضع للإشراف: يحتوي هذا النوع على عملية تدريب بمجموعة كبيرة من البيانات المعنونة. بعد عملية التدريب؛ يجب فحص النظام بمجموعة بيانات الاختبار. عادة ما تستخدم خوارزميات التعلم هذه كآلية تصنيف أو آلية انحدار. تقوم خوارزمية الانحدار بإنشاء مخرجات أو قيم تنبؤ، وهي رقم واحد أو أكثر من الأرقام ذات القيمة المستمرة وفقًا للإدخال. تصنّف خوارزميات التصنيف البيانات إلى فئات وعلى عكس آلية الانحدار، فإنّ خوارزميات التصنيف تولّد مخرجات منفصلة.

• التعلّم غير الخاضع للإشراف: على عكس التعلّم الخاضع للإشراف، يستخدم التعلّم غير الخاضع للإشراف مجموعة بيانات تدريب غير مسمّاة. عادةً ما يُستخدم التعلّم غير الخاضع للإشراف لتجميع البيانات أو تقليل الأبعاد أو تقدير الكثافة.

• التعلم المعزّز: يتعلّم هذا النوع من خوارزمية التعلّم أفضل الإجراءات بناءً على المكافآت أو العقوبات. يمكن عدّ التعزيز مزيجاً من التعلّم الخاضع للإشراف والتعلّم غير الخاضع للإشراف. التعلّم المعزّز مفيد في الحالات التي تكون فيها البيانات محدودة أو غير معطاة.

1-3- خوارزميات التصنيف (Classification)

نوضّح فيما يلي مجموعة من خوارزميات التي يمكن تجربتها كمسألة تصنيف. سيتم استخدام مشكلة تصنيف التعلم الآلي القياسية لتوضيح كل خوارزمية.

1-3-1- Logistic Regression (الانحدار اللوجستي): هي خوارزمية تصنيف ثنائي. تفترض أن متغيرات الإدخال رقمية ولها توزيع غاوسي (منحنى الجرس). في حالة مجموعة بيانات Ionosphere، تحتوي بعض سمات الإدخال على توزيع شبيه بتوزيع Gaussian، لكن العديد منها لا يفعل ذلك. تتعلم الخوارزمية عنصرًا ثابتًا لكل قيمة إدخال، والتي تُدمج خطياً في دالة انحدار وتحويلها باستخدام تابع (على شكل s). يعد الانحدار اللوجستي أسلوبًا سريعًا وبسيطًا، ولكنه يمكن أن يكون فعالاً لحلّ العديد من المشكلات.

1-3-2- Naive Bayes هي خوارزمية تصنيف. تفترض تقليدياً أنّ قيم المدخلات اسمية، على الرغم من أن المدخلات العددية مدعومة بافتراض التوزيع. يستخدم Naive Bayes تطبيقاً بسيطاً لنظرية بايز (ومن ثم فهو ساذج) إذ يُحسب الاحتمال السابق لكل فئة من بيانات التدريب ويفترض أنّه مستقلّ عن بعضهما البعض (يُطلق عليه تقنياً الاستقلال الشرطي). يعدّ ذلك افتراض غير واقعي لأننا نتوقّع أن تتفاعل المتغيّرات وتكون تابعة، على الرغم من أن هذا الافتراض يجعل الاحتمالات سريعة وسهلة الحساب. حتى في ظل هذا الافتراض غير الواقعي، فقد ثبت أنّ Naive Bayes هي خوارزمية تصنيف فعالة للغاية.

يحسب Naive Bayes الاحتمال اللاحق لكلّ فئة ويقوم بالتنبؤ للفئة ذات الاحتمال الأعلى. وهو يدعم كلّاً من مشاكل التصنيف الثنائي والتصنيف متعدد الفئات.

1-3-3- Decision Tree: يمكن أن تدعم أشجار القرار مشاكل التصنيف والانحدار. يشار مؤخراً إلى أشجار القرار باسم أشجار التصنيف والانحدار (CART). تعمل عن طريق إنشاء شجرة لتقييم مثيل(instance) من البيانات. تتقلّب الشجرة بدءاً من أعلى أو جذر الشجرة ثم تتحرك نزولاً إلى الأوراق حتى يمكن التنبؤ. تعمل عملية إنشاء شجرة قرار عن طريق الاختيار الجشع (Greedy) لأفضل نقطة تقسيم من أجل عمل تنبؤات وتكرار العملية حتى تصبح الشجرة ذات عمق ثابت. بعد إنشاء الشجرة، تُقتطع لتحسين قدرة النموذج على التعميم على البيانات الجديدة. تعد خوارزمية C4.5 خوارزمية شجرة القرار الأخرى الأكثر تقدماً.

1-3-4- k-Nearest Neighbors: تدعم خوارزمية k- الأقرب للجيران كلاً من التصنيف والانحدار. يطلق عليه أيضًا KNN للاختصار. تعمل عن طريق تخزين مجموعة بيانات التدريب بالكامل والاستعلام عنها لتحديد أنماط التدريب الأكثر تشابهاً عند إجراء التنبؤ. بهذه الطريقة، لا يوجد نموذج آخر غير مجموعة بيانات التدريب الأولية والحساب الوحيد الذي يتم إجراؤه هو الاستعلام عن مجموعة بيانات التدريب عند طلب التنبؤ.

تعدّ خوارزمية بسيطة ولكنها لا تفترض الكثير عن المشكلة بخلاف أن المسافة بين مثيلات البيانات ذات أهمية في عمل التنبؤات. وبالتالي فإنها غالباً ما تحقّق أداءً جيدًا جدًا. عند إجراء تنبؤات حول مشاكل التصنيف، ستأخذ KNN الوضع (الفئة الأكثر شيوعًا) لأكثر الحالات المماثلة في مجموعة بيانات التدريب.

1-3-5- Support Vector Regression (SVR): تم تطوير آلات المتجهات الداعمة لمشاكل التصنيف الثنائي ، على الرغم من أنه تم إجراء امتدادات لهذه التقنية لدعم مشاكل التصنيف والانحدار متعدد الفئات.
طُوّرت SVM لمتغيّرات الإدخال الرقمية، وبالتالي فأنّه يتم تحويل القيم الاسمية إلى قيم عددية. يتم أيضاً تطبيع بيانات الإدخال قبل استخدامها.
على عكس SVM الذي يعثر على سطر يفصل بيانات التدريب بشكل أفضل إلى فصول، يعمل SVR عن طريق العثور على سطر من أفضل t ممّا يقلّل من خطأ دالة التكلفة. يتم ذلك باستخدام عملية تحسين تراعي فقط مثيلات البيانات الموجودة في مجموعة بيانات التدريب الأقرب إلى السطر بأقل تكلفة. تسمى هذه الحالات متجهات الدعم، ومن هنا جاء اسم التقنية.

أهميّة البحث وأهدافه:

أصبحت المبادرات المتعلقة بالمركبات المتصلة والمستقلة (CAV) من أسرع المبادرات توسعاً في السنوات الأخيرة ، وبدأت في التأثير على الحياة اليومية للأشخاص. أعلنت المزيد والمزيد من الشركات والمؤسسات البحثية عن مبادراتها. كما أدخلت الحكومات في جميع أنحاء العالم سياسات لدعم وتسريع نشر CAVs. إلى جانب ذلك، أصبحت قضايا مثل الأمن السيبراني في CAV هي السائدة وتشكل جزءاً أساسياً من تعقيدات نشر CAV. ومع ذلك ، لا يوجد عالميا إطار عمل متفق عليه أو معترف به للأمن السيبراني CAV.
يهدف البحث إلى مقارنة أداء خوارزميات تعلّم الآلة للحماية من الهجمات السيبرانية من حيث الدقة وزمن التشغيل على مجموعة بيانات جديدة معدّلة عن مجموعة البيانات KDD99.

1- الدراسات المرجعيّة

في [3] تمّ تحليل التهديدات على المركبات الآلية المستقلّة والمركبات الآلية التعاونية. يُظهر هذا التحليل الحاجة إلى المزيد من التكرار بشكل أكبر ممّا توقّعه الكثيرون. قام أيضاً برفع مستوى التركيز لإثارة النقاش حول هذه التهديدات في هذه المرحلة المبكرة من تطوير أنظمة أتمتة المركبات. وخلص إلى أنّ انتحال نظام GNSS وحقن رسائل مزيفة من أخطر التهديدات السيبرانية.

في [4] تمّ تقسيم الهجمات الإلكترونية عبر الإنترنت إلى نوعين رئيسيين: الهجمات السلبية والهجمات النشطة. يصعب التعرّف على الهجمات السلبية ولكن من السهل الدفاع عنها، إذ لا يتفاعل المهاجمون مع البيانات؛ بينما من السهل التعرّف على الهجمات النشطة، مثل التعديل والانتحال، ولكن يصعب الدفاع عنها، إذ يمكن للمهاجمين تعديل أو تزوير الرسائل في نقل البيانات. حالياً، لا يوجد معيار أمان عالمي حالي لمركبات CAVs. وبالتالي، فإنّ التعريف المنهجي لطرق تحليل الهجمات أمر مرغوب فيه للغاية لتطوير CAVs.
في [5] تمت الإشارة إلى أنّ معيار سلامة المركبات الحالي ISO26262 لا يأخذ بالحسبان القضايا الأمنية لتجنّب كلّ من الهجمات غير المقصودة والمتعمّدة.
في [6]، تمّ تقديم نظرة عامة وعميقة على التحدّيات المختلفة المرتبطة بتطبيق التعلّم الآلي في شبكات المركبات، والتركيز على منظور هجمات ML المعادية علىCAVs وتحديد حلّ للدفاع ضدّ الهجمات العدائية في أماكن متعدّدة.
في [7] اقتُرح التعلّم الآلي الموجّه كبروتوكول محدد لمكافحة التشويش لبيئات حركة مرور المركبات من خلال التركيز على الكشف عن الإشارات المميزة للمركبة وترشيحها للكشف عن الموقع الدقيق للمركبات المتأثرة بالتشويش. يتم

استخدام عامل ترشيد لفحص تغيرات التردد الناتجة في قوة الإشارة بسبب التشويش أو الهجمات الخارجية. تم استخدام خوارزمية التعلّم الآلي مفتوحة المصدر "CatBoost" مع التركيز على الخوارزمية المعتمدة على شجرة القرار للتنبؤ بمواقع مركبة التشويش. يشهد التقييم على الخصائص المقاومة لتقنية مكافحة التشويش مع مراعاة الدقّة والتذكّر ودرجة F1 ومقاييس دقّة التسليم. استنتج أنّ المخطط القائم على التعلم الآلي يعمل بشكل فعّال ضدّ هجمات التشويش على موقع CAV.

وفقًا لمسح أجري في جامعة ميشيغان [8]، يكون الاهتمام أكثر بالأضرار المادية التي تسبّبها CAVs أكثر من تسرّب المعلومات الخاصّة. ومع ذلك، فقد وجد أنّه لا يوجد ما يكفي من الأعمال ذات الصلة بشأن الأمن السيبراني الخاص بشبكات CAVs.

زوّدت وكالة الفضاء الأوروبية (ESA) مؤخراً دعوةً لتقديم مقترحات بشأن حلول CAV للأمن السيبراني باستخدام الذكاء الاصطناعي [9]. وفي [16] حدّد الباحثون مبادئ الأمن السيبراني لشبكات CAVs في المملكة المتّحدة.

طرائق البحث ومواده:

نستخدم في هذا البحث مجموعة بيانات (data set) مشتقة من مجموعة البيانات KDD99 [20] بحيث تكون مخصّصة لاكتشاف الهجمات وتحقيق الأمن في شبكات CAVs. إذ تحتوي مجموعة البيانات الجديدة على 14 نوعاً من الهجمات الفرعية التي تهدّد CAVs.

بعد إزالة التكرارات وأنواع الهجمات غير المرتبطة بشبكات CAVs، تمّ إنشاء مجموعة بيانات جديدة متوافقة مع إطار عمل الأمن السيبراني CAV الجديد. يعرض الجدولان 1 و2 كمية البيانات العادية وبيانات الهجوم في كل من مجموعات بيانات التدريب.

جدول1 : مقدار البيانات العادية وبيانات الهجوم في مجموعات بيانات التدريب.

	10% KDD Data	New Data
Attacks	396.743	54.485
Normal	97.278	87.832
Total	494.021	142.317

جدول2 : مقدار البيانات العادية وبيانات الهجوم في مجموعات بيانات التدريب.

	10% KDD Test Data	New Test Data
Attacks	250.436	23.348
Normal	60.593	47.913
Total	311.029	71.261

نقوم بمقارنة أداء خوارزميتي تعلّم الآلة Decision Tree و Naive Bayes على مجموعة البيانات الجديدة من حيث الدقّة وزمن التشغيل اللازم باستخدام الأداة WEKA.

2- أنواع الهجمات في KDD99

تحتوي مجموعة بيانات KDD99 على أكثر من 4 ملايين سجل بيانات، وهي كبيرة جداً لمعالجة البيانات على أجهزة الحاسوب الشخصية. في هذا البحث، استخدمت مجموعة بيانات التدريب مع 10٪ من مجموعة بيانات KDD99.

تنقسم الهجمات في KDD99 إلى أربعة أنواع رئيسية مع 39 هجوماً فرعياً وهي على النحو التالي [21]:

1. فحص (PROBE)، هذا النوع من الهجوم يفحص النظام بحثاً عن نقاط الضعف لجمع المعلومات من النظام. في KDD99، تشمل الهجمات الفرعية لهذا النوع: ipsweep و mscan و nmap و ortsweep و saint و satan.

2. هجوم DoS (رفض الخدمة)، يعطّل الاستخدام العادي أو الاتّصال في النظام من خلال احتلال جميع الموارد، بحيث لا يكون النظام أو قناة الاتصال متاحة للاستخدام العادي. عادةً، يرسل المهاجمون كمية هائلة من البيانات لإغراق قناة ونظام الاتصال. في KDD99، تحتوي هجمات DoS على apache2 و back و land و mailbomb و Neptune و pod و processtable و smurf و teardrop و udpstorm.

3. هجوم U2R (مستخدم إلى جذر). يهدف المهاجمون إلى الوصول إلى حسابات المستخدم المتميز. يكتشفون نقاط الضعف في النظام ثم يحصلون على حق الوصول إلى جذر النظام. في KDD99، تتضمّن هجمات U2R buffer_overflow و HTptunnel و loadmodule و perl و ps و rootkit و sqlattack و xterm.

4. هجوم R2L (من بعيد إلى محلي). يهدف المهاجمون إلى الوصول إلى النظام وإرسال الحزم باستخدام اتصال بعيد. لا يمتلك المهاجم حساباً مصرّحاً به في النظام، ولكن يمكنه الوصول إليه محليّاً.

في KDD99 ، تحتوي هذه الملفّات على ftp_write ، و guess_passwd ، و imap ، و multihop ، و phf ، وإرسال بريد، و snmpgetattack ، و snmpguess ، و spy ، و Warezclient ، و warezmaster ، و worm ، و xlock ، و xsnoop.

يوفّر KDD99 مجموعة بيانات شاملة تغطّي مجموعة متنوعة من أنواع الهجمات في شبكات الكمبيوتر. ومع ذلك، لا يمكن استخدام مجموعة البيانات مباشرة للأمن السيبراني CAV ، بسبب الخصائص المميزة لـ CAVs المذكورة أعلاه. في هذا البحث، نقوم بتكييف مجموعة بيانات KDD99 ومعالجتها عن طريق إزالة أنواع الهجمات غير المرتبطة.

يعرض الجدول3 أنواع الهجمات المحتملة في KDD99 والتي قد تحدث أيضاً في CAV. في الجدول 3، صُنّفت الأنواع المحتملة لهجمات CAV إلى ثلاثة مستويات: H لـ High و P لـ Possible و I للهجمات غير المرتبطة (Irrelevant). بعد معالجة البيانات، انخفض العدد الإجمالي لأنواع هجمات CAV من 39 إلى 14، مع 19 نوعاً من هجوم CAV محتمل و 6 أنواع من الهجوم غير ذي الصلة.

يمكن تبرير معالجة البيانات على أنواع الهجمات المختلفة وفق الشكل السابق على النحو التالي:

1. كانت بعض الهجمات بدون تعريف واضح. نظراً لأنّ البيانات مأخوذة من مجموعة بيانات KDD99، فإنّ تعريفات الهجمات تشير إلى أوصافها الأصلية. تفتقر بعض الهجمات الفرعية إلى تعريفات واضحة، وبالتالي لا يمكن تصنيفها على أنها من النوع P في هجمات CAV. يمكن تغيير نوع الهجوم بمجرّد توفّر تعريف واضح.

2. لا تنسجم بعض الهجمات مع إطار عمل الأمن السيبراني CAV. ومع ذلك؛ نظراً لأن KDD99 عبارة عن مجموعة بيانات حول أمان الحاسوب والشبكة، فإنّ بروتوكولاتها تختلف عن تلك الموجودة في CAVs. على سبيل المثال، في KDD99 ، يحدث الهجوم "land" فقط في بروتوكولات TCP/IP الأقدم، ويمكن العثور عليه فقط في نظام تشغيل Linux قديم يسمى SunOS 4.1.

بمجرّد انتهاء صلاحية البروتوكول والبيئة، قد تختفي أيضاً إمكانية حدوث هذا الهجوم. لا تتناسب هذه الأنواع من الهجمات مع إطار عمل CAV، لذا تمت إزالتها.

3. لم تكن بعض الهجمات متوافقة مع نقاط هجوم CAV. لإجراء هجوم، باستثناء الضرر المادي، يحتاج المهاجمون إلى العثور على إحدى النقاط الضعيفة في نظام CAV. يمكن أن تكون نقاط الهجوم هذه في أجزاء مادية أو برامج أو بيانات أو قناة اتصال.

جدول 3: هجمات KDD99 الفرعية الممكنة في شبكات CAVs.

	Attack Type	Possibility		Attack Types	Possibility
PROBE	ipsweep	H	U2R	ps	I
	mscan	P		rootkit	P
	nmap	H		sqlattack	P
	portsweep	P		xterm	I
	Saint	P	R2L	ftp_write	H
	satan	P		gues_passwd	H
DOS	apache2	P		imap	I
	back	P		multihop	P
	land	P		named	P
	mailbomb	H		phf	I
	neptune	H		sendmail	P
	pod	H		snmpgetattack	P
	processtable	P		snmpguess	P
	smurf	H		spy	P
	teardrop	H		warezclient	P
	udpstorm	H		warezmaster	P
U2R	buffer_overflow	H		worm	H
	httptunnel	H		xlog	P
	loadmodule	I		xsnoop	H
	perl	I			

في KDD99، يمكن أن تحدث بعض الهجمات فقط في ظلّ ظروف ومنصّات محدّدة، وبالتالي لا تنطبق على نقاط هجوم CAV. احتمالات هذه الهجمات في CAV منخفضة؛ على سبيل المثال، يمكن أن يحدث هجوم apache2 فقط في مخدّم ويب Apache. إذا كان CAV لا يستخدم مخدّم الويب Apache فلا يمكن تنفيذ الهجوم.

النتائج والمناقشة:

استُخدمت خوارزميتا تعلّم آلة تمّ تطويرهما على المحاكي WEKA لبناء نماذج التصنيف، الأولى هي Naïve Byes والثانية هي Decision Tree لاكتشاف الشذوذ في البيانات. نُفّذت التجارب على جهاز Intel Core 2Duo, 2 GHz مع نظام تشغيل windows7 64bit.

تعدّ WEKA أداة مفتوحة المصدر للتنقيب عن البيانات طوّرتها جامعة Waikato واستخدمت بشكل واسع في الأبحاث والدراسات اللازمة لتحليل وتطوير نماذج تعلّم الآلة.

بعد معالجة بيانات KDD99 الأصليّة، خُفّض عدد أنواع الهجوم إلى 14. استخدمت مجموعة البيانات الجديدة لبناء نماذج الكشف، والتي تم اختبارها على مجموعة بيانات الاختبار. تستخدم مجموعة التدريب أولاً التحقّق من صحّة 10 أضعاف 10-folds cross validation لبناء النموذج. ثم يتم التحقق من صحة نموذج التعلم الآلي في مجموعة

بيانات اختبار. تقارن الدقة الشاملة ووقت التشغيل لنماذج شبكة Decision Tree وNaive Bayes في الجدول 3. تشير الدقّة إلى نسبة الهجمات المصنّفة الصحيحة إلى العدد الإجمالي للتصنيف.

جدول 3: الدقّة ووقت التشغيل لخوارزميتي تعلّم الآلة على بيانات الاختبار

	Accuracy on the Testing Data Set	Time to Build Model(s)	Time on the Testing Data Set(s)
Naïve Byes	85.8%	0.06	3.2
Decision Tree	93.9%	0.59	0.4

من الجدول 3 يمكن ملاحظة أن نموذج شجرة القرار حقّق دقّة أعلى من نموذج Naïve Byes، بينما اختلف وقت التشغيل. في بيئة القيادة في الزمن الحقيقي خاصةً عندما تسير مركبات CAVs بسرعة عالية، إذ يمكنها قطع مسافة طويلة تزيد عن 30 متراً في أقلّ من ثانية، نلاحظ أنّ Naive Bayes استغرقت وقتاً أطول لتحديد الهجمات (العمود الأخير)، لذا كانت Decision Tree أكثر كفاءة للأمن السيبراني في CAVs.

بالإضافة إلى ذلك، نظراً للخصائص المميّزة لـ CAVs، فإنّ معدّل تصنيف الهجوم الإيجابي الخاطئ (FP) يعدّ أيضًا مقياساً مهمّاً لتقييم أداء النماذج. في بيئة العالم الحقيقي، قد تكون العواقب خطيرة إذا صنّف نموذج التعلم الآلي بيانات الهجوم على أنّها بيانات عادية. بناءً على ذلك، يظهر الجدول4 المعدّل الإيجابي الخاطئ FP.

يمكن ملاحظة أنه مع التحقّق من الصحّة 10 أضعاف (10-folds cross validation)، إذ تم تحليل جميع أنواع الهجمات وتدريبها. يتشابه المعدل الإيجابي الخاطئ لكلا النموذجين في مجموعة بيانات الاختبار ويحقّقان دقّة جيدة. بناءً على هذه النتائج، يعدّ المعدل الإيجابي الخاطئ مقبولاً لكلا النموذجين.

جدول 4: المعدّل الإيجابي الخاطئ لـ J48 و Naive Byes.

	TP Rate on the Testing Data Set	FP Rate on the Testing Data Set	Precision on Testing Data Set
Naïve Byes	81.1%	22.5%	85.8%
J48	94%	22.2%	93.9%

من خلال إعادة النتائج السابقة على مجموعة بيانات مختزلة عن KDD99 بنسبة 20 بالمئة، يمكن الحصول على النتائج الموضّحة في الجدول5.

جدول5: المعدّل الإيجابي الخاطئ لـ J48 و Naive Byes.

	TP Rate on the Testing Data Set	FP Rate on the Testing Data Set	Precision on Testing Data Set	Time to build the model
Naïve Byes	96.6%	3.8%	96.7%	0.19
J48	98.3%	1.8%	98.3%	1.58

جدول6: النتائج لكل نوع من انواع الهجمات.

	DT FP Rate	NB FP Rate	DT accuracy	NB accuracy
PROBE	0.18%	0.81%	98.3%	92.7%
DoS	0.4%	1.06%	99.6%	89.6%
R2L	0.18%	1.06%	98.3%	89.6%
U2R	0.4%	1.06%	99.6%	89.6%

من الجدول 6، يمكن ملاحظة أن كلا نموذجي تصنيف التعلم الآلي يتمتعان بدقّة عالية. كانت المعدلات الإيجابية الخاطئة منخفضة في جميع بيانات الهجوم. عند تحديد هجمات PROBE ، كان أداء DT ممتازاً أفضل من أداء NB. عند تحديد هجمات DoS، كانت دقّة شجرة القرار أعلى بكثير. كان أداء نموذج شجرة القرار أيضاً أفضل في هجمات U2R و R2L.

بناءً على النتائج السابقة، يمكن القول أنّ خوارزمية شجرة القرار حقّقت نتائج أفضل فيما يتعلّق بالهجمات القائمة على الاتصالات في بيئة CAV. إذ يمكن لنموذج شجرة القرار اكتشاف الهجوم في وقت قصير بدقة جيّدة. ومع ذلك، يجب أيضاً ملاحظة أن كلا النموذجين قد حصلوا على نتائج غير مرضية عند التنبؤ بهجمات غير مرئية، الأمر الذي يحتاج إلى مزيد من الدراسات في الأعمال المستقبلية.

الاستنتاجات والتوصيات:

تعدّ شبكات CAVs من المواضيع الهامة، وبسبب خصائصها المتمثّلة في الاتصال اللاسلكي وذاتيّة القيادة فإنّها تكون معرّضة لأنواع مختلفة من الهجمات. وضّح البحث كيفيّة استخدام تقنيات الذكاء الاصطناعي لكشف أربعة أنواع من الهجمات من خلال المقارنة بين خوارزميتي Naïve Byes وشجرة القرار. تبيّن من خلال النتائج التي تمّ التوصّل إليها أن خوارزمية شجرة القرار أكثر دقّة في التصنيف.

من الممكن دراسة تقنيات أخرى لكشف أنواع أخرى أيضاً من الهجمات وخاصّة الهجمات التي تكون غير مرئية بالنسبة للتقنيات التي تمت دراستها.

References:

[1] Guerra, E. Planning for cars that drive themselves: Metropolitan Planning Organizations, regional transportation plans, and autonomous vehicles. J. Plan. Educ. Res. 2016, 36, 210–224.

[2] Gov.UK. Center for Connected and Autonomous Vehicles. 2018. Available online: https://www.gov.uk/government/organisations/centre-for-connected-and-autonomous-vehicles (accessed on 9 December 2018).

[3] Petit, J.; Shladover, S.E. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. 2015, 16, 546–556.

[4] He, Q.; Meng, X.; Qu, R. Survey on cyber security of CAV. In Cooperative Positioning and Service (CPGPS); IEEE: Harbin, China, 2017; pp. 351–354.

[5] Integrating Autonomous Vehicle Safety and Security, 2017. Available online: https://www.researchgate.net/publication/321323032_Integrating_Autonomous_Vehicle_Safety_and_Security (accessed on 10March 2022).

[6] Qayyum, A.; Usama, M.; Qadir, J.; Al-Fuqaha, A. Securing Connected Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and theWay Forward. IEEE Commun. Surv. Tutor. 2020, 22, 998–1026.

[7] Kumar, S.; Singh, K.; Kumar, S.; Kaiwartya, O.; Cao, Y.; Zhou, H. Delimitated Anti Jammer Scheme for Internet of Vehicle: Machine Learning based Security Approach. IEEE Access 2019, 7, 113311–113323.

[8] Cybersecurity Concerns with Self-Driving and Conventional Vehicles, 2017. Available online: http://umich.edu/~umtriswt/PDF/SWT-2017-3.pdf (accessed on 26 March 2019).

[9] Cyber Security and Space Based Services—ESA Business Applications, 2019.

Available online: https://business.esa.int/funding/invitation-to-tender/cyber-security-and-space-based-services (accessed on 31 May 2022).
[10] Hall, M.; Frank, E.; Holmes, G.; Pfahringer, B.; Reutemann, P.; Witten, I.H. The WEKA data mining software: An update. ACM SIGKDD Explor. Newsl. 2009, 11, 10–18.
[11] Arockia Panimalar.S, GiriPai.U, Salman Khan.K, "ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue:03 | Mar-2018, e-ISSN: 2395-0056, p-ISSN: 2395- 0072.
[12] [Chung, S. (2021). AI-Based CYBERSECURITY: Benefits and Limitations.]
[13] [Ansari, Dash, Sharma, &Yathiraju. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review.
https://www.researchgate.net/publication/364122631_The_Impact_and_Limitations_of_Artificial_Intelligence_in_Cybersecurity_A_Literature_Review]
[14] Das, Rammanohar & Sandhane, Raghav. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series. 1964. 042072. 10.1088/1742-6596/1964/4/042072.
[15] Atiku, Shidawa.B., Aaron, Achi.U., Job, Goteng.K., Shittu, Fatima, Yakubu, Ismail.Z. (2020). Survey On The Applications Of Artificial Intelligence In Cyber Security, International Journal of Scientific & Technology Research, 9,10, 165-170
[16] GOV.UK. The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles. 2017. Available online: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-andautomated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles (accessed on 6 August 2022).
[17] The Pathway to Driverless Cars Summary Report and Action Plan. 2018. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf (accessed on 6 August 2022).
[18] Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Trans. Intell. Transp. Syst. 2017, 18, 2898–2915.
[19] Schatz, D.; Bashroush, R.;Wall, J. Towards a more representative definition of cyber security. J. Digit. Forensics Secur. Law. 2017, 12, 8.
[20] UCI kdd cup 1999 Data Data Set, 1999. Available online: https://archive.ics.uci.edu/ml/datasets (accessed on 1 June 2022).
[21] Arora, I.S.; Bhatia, G.K.; Singh, A.P. Comparative Analysis of Classification Algorithms on KDD'99 Data Set. Int. J. Comput. Netw. Inf. Secur. 2016, 8, 34.