

قضايا بحثية ٣ – الأسبوع (العاشر)

تقرير أكاديمي حول المهمة العاشرة: (ملخص تنفيذي
لأحدى الدراسات)
في مجال التخصص "تقنية المعلومات"

إعداد الطالب/
عبد السلام العتيبي

٢٠٢٥م



ملخص تنفيذي

عنوان المشروع: مخطط فعال لكشف التسلل في الوقت
الفعلي داخل شبكات المركبات باستخدام التعلم التجميعي.

المؤلف: عيسى العلواني (Easa Alalwany)

جهة النشر: جامعة فلوريدا أتلانتيك (Florida Atlantic
University)، رسالة دكتوراه، ديسمبر ٢٠٢٣

١. إشكالية البحث وأهدافه

مع التطور الهائل في صناعة السيارات واعتمادها المتزايد على الأنظمة الإلكترونية المتصلة، أصبحت شبكات المركبات الداخلية، وعلى رأسها شبكة CAN bus، عرضة بشكل كبير للتهديدات السيبرانية. تكمن الإشكالية في أن بروتوكول CAN، الذي يُعد العمود الفقري للاتصالات داخل المركبة، قد صُمم في الأصل دون وجود آليات أمنية أساسية مثل التشفير أو المصادقة. هذا القصور الأمني يجعل المركبات عرضة للاختراقات التي قد تتيح للمهاجمين التحكم في وظائف حيوية مثل نظام الفرامل، المحرك، أو التوجيه، مما يهدد بشكل مباشر سلامة السائقين والركاب. في ضوء هذا الخطر المتزايد.

١. إشكالية البحث وأهدافه

يهدف هذا المشروع البحثي إلى تصميم وتطوير مخطط فعال لكشف التسلل (Intrusion Detection Scheme) يعتمد على أحدث تقنيات التعلم الآلي، وتحديدًا التعلم التجميعي (Ensemble Learning)، بهدف تحقيق دقة وسرعة فائقتين في اكتشاف وتصنيف الهجمات السيبرانية داخل شبكات المركبات في الوقت الفعلي.

٢. المنهجية المتبعة

لتحقيق أهدافه، اتبع الباحث منهجية علمية دقيقة وشاملة تتضمن عدة مراحل:

. **جمع ومعالجة البيانات:** تم الاعتماد على مجموعة بيانات حقيقية وشاملة لشبكة CAN من (IEEE DataPort). تم اختيار هذه المجموعة لقربها من الواقع وشمولها لأنواع متعددة من الهجمات الشائعة مثل هجمات الحرمان من الخدمة (DoS)، وهجمات التشويش (Fuzzing)، وهجمات إعادة التشغيل (Replay)، وهجمات الانتحال (Spoofing). لمعالجة مشكلة عدم التوازن في البيانات، حيث تكون رسائل الهجوم أقل بكثير من الرسائل العادية، تم استخدام تقنية Oversampling وهي طريقة لإنتاج عينات إضافية من فئة الأقلية لضمان أن النماذج لا تتحيز للفئة الأكبر.

٢. المنهجية المتبعة

١. تطوير النماذج: تم اختبار ثماني خوارزميات تعلم آلي إشرافي فردية، مثل Naive Bayes و SVM و K-NN، بشكل منفصل لتحديد أفضلها أداءً. بعد ذلك، تم دمج هذه النماذج في مجموعات باستخدام ثلاث طرق تجميعية قوية: التصويت (Voting)، والتكديس (Stacking)، والتجميع (Bagging). يمثل التعلم التجميعي نهجاً أكثر تطوراً يجمع بين تنبؤات نماذج متعددة لإنشاء تنبؤ نهائي أكثر دقة وموثوقية، مما يقلل من نقاط ضعف كل نموذج على حدة.

٢. الكشف في الوقت الفعلي: تم تصميم المخطط بحيث يكون قابلاً للتطبيق في بيئة حية. ولتحقيق ذلك، تم دمجه مع هندسة Kappa، وهي بنية معالجة بيانات تتيح معالجة تدفقات البيانات الضخمة في الوقت الفعلي (stream processing) بفعالية. بالإضافة إلى ذلك، تم الاستفادة من قوة إطار عمل Apache Spark لمعالجة البيانات الضخمة بكفاءة عالية، مما يضمن أن النموذج قادر على تحليل البيانات الواردة بشكل مستمر واتخاذ القرارات في الوقت المناسب.

٣. النتائج الرئيسية والمساهمة

أثبتت نتائج الدراسة بشكل قاطع أن النماذج التجميعية تفوقت بشكل ملحوظ على النماذج الفردية في جميع مقاييس الأداء. وقد حققت طريقة التكديس (Stacking) أعلى دقة إجمالية، حيث وصلت إلى ٩٨.٥٦% في الكشف عن الهجمات وتصنيفها. هذا الأداء المتميز يبرهن على أن دمج تنبؤات النماذج الفردية يمكن أن يؤدي إلى تحسين كبير في الكفاءة. كما تفوقت النماذج التجميعية في مقاييس مهمة مثل الشمول (Recall) ودرجة F1، مما يؤكد فعاليتها في كشف الهجمات بدقة مع تقليل الإنذارات الكاذبة.

تساهم هذه الدراسة بشكل كبير في مجال الأمن السيبراني للمركبات من خلال تقديم:

- مخطط تنبؤي موثوق يمكنه العمل بكفاءة في الوقت الفعلي، وهو أمر بالغ الأهمية لتوفير حماية فورية.

- إثبات عملي لأهمية وفاعلية التعلم التجميعي في مواجهة التحديات الأمنية المعقدة.
- منهجية شاملة وقابلة للتكرار يمكن استخدامها كأساس لتطوير أنظمة كشف تسلل مستقبلية.

٤. الخاتمة

يقدم هذا المشروع البحثي حلاً واعدًا لمواجهة التحديات الأمنية المتزايدة في شبكات المركبات الحديثة. إن المخطط المقترح، الذي يجمع بين قوة التعلم التجميعي وكفاءة المعالجة في الوقت الفعلي، يمهد الطريق لتطوير أنظمة أمنية أكثر فعالية وموثوقية في قطاع صناعة السيارات. هذه الدراسة لا تفتح آفاقاً جديدة للبحث الأكاديمي فحسب، بل تقدم أيضاً إطاراً عملياً يمكن للمهندسين والمطورين الاستفادة منه لتعزيز أمان المركبات، مما يضمن في نهاية المطاف سلامة السائقين والركاب في المستقبل.

المرجع

Alalwany, E. (2023). An effective ensemble learning-based real-time intrusion detection scheme for in-vehicle network (Doctoral dissertation, Florida Atlantic University).



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

