

دراسات نقدية ٣ – الأسبوع (العاشر)

تقرير نقدي حول المهمة العاشرة: (النقد الموضوعي)
لأطروحة دكتوراه لأحد زملاء التخصص
"تقنية المعلومات"

إعداد الطالب/
عبد السلام العتيبي

٢٠٢٥م



بيانات الدراسة (موضع النقد)

البيانات	المحتوى	ترجمة المحتوى للعربية
عنوان الدراسة	AN EFFECTIVE ENSEMBLE LEARNING-BASED REAL-TIME INTRUSION DETECTION SCHEME FOR IN-VEHICLE NETWORK	مخطط فعال لكشف التسلل في الوقت الفعلي داخل شبكات المركبات باستخدام التعلم التجميعي.
اسم المؤلف	Easa Alalwany	عيسى العلواني.
سنة النشر	December 2023	ديسمبر ٢٠٢٣.
جهة النشر	Florida Atlantic University (Dissertation)	جامعة فلوريدا أتلانتيك (رسالة دكتوراه).
التوثيق وفق نظام APA7	Alalwany, E .(٢٠٢٣) .An effective ensemble learning-based real-time intrusion detection scheme for in-vehicle network) Doctoral dissertation, Florida Atlantic University.(	العلواني، ع. (٢٠٢٣). مخطط فعال لكشف التسلل في الوقت الفعلي داخل شبكات المركبات باستخدام التعلم التجميعي (رسالة دكتوراه غير منشورة). جامعة فلوريدا أتلانتيك.

مقدمة

يهدف هذا التقرير إلى تقديم قراءة نقدية معمقة لرسالة دكتوراه بعنوان "مخطط فعال لكشف التسلل في الوقت الفعلي داخل شبكات المركبات باستخدام التعلم التجميعي"، والتي تتدرج ضمن مجال تكنولوجيا المعلومات وتطبيقاتها في الأمن السيبراني. يركز التقييم على تحليل جوانب الدراسة من حيث القوة والضعف، وتقديم توصيات بناءة تساهم في تطوير الأبحاث المستقبلية في هذا المجال الحيوي.

١. نقاط القوة في الدراسة

تتميز الدراسة بعدة جوانب إيجابية تعكس جهدًا بحثيًا كبيرًا وعمقًا في فهم المشكلة، من أبرزها:

. **أصالة الموضوع وأهميته:** تتناول الدراسة مشكلة حيوية ومتنامية الأهمية في مجال تقنية المعلومات، وهي الأمن السيبراني في قطاع المركبات الحديثة. إن الاعتماد المتزايد على شبكات CAN يجعل المركبات عرضة للهجمات، مما يهدد سلامة الركاب. يسلط البحث الضوء على الحاجة الماسة لنظم كشف تسلل فعالة في بيئة محدودة الموارد.

. **تحديد المشكلة والهدف بوضوح:** تحدد الدراسة مشكلتها بوضوح، حيث تبرز أن بروتوكول CAN يفتقر إلى آليات أمان أساسية مثل التشفير والمصادقة، مما يتطلب تطوير نظم كشف تسلل دقيقة. وتقدم حلاً منهجيًا وموسعًا يهدف إلى تحسين دقة وكفاءة نظم كشف التسلل باستخدام التعلم التجميعي.

١. نقاط القوة في الدراسة

. المنهجية العلمية والتحليلية: تميزت الدراسة بمنهجية قوية وخطوات واضحة، بدءًا من معالجة البيانات الأولية مثل تنقية البيانات (Data Cleaning) والموازنة بين الفئات (Data Balancing) باستخدام تقنية Oversampling لمعالجة مشكلة عدم التوازن في بيانات الهجمات. كما قامت الدراسة بتقييم الأداء بناءً على مقاييس دقيقة مثل الدقة (Accuracy)، والشمول (Recall)، ودرجة F1 (F1-Score)، ومساحة تحت منحنى ROC (ROC-AUC).

. الاستخدام الفعال لنماذج التعلم العميق والتجميعي: أظهرت الدراسة فهمًا عميقًا لنماذج التعلم الآلي، حيث قامت بتجربة ثماني خوارزميات إشرافية مختلفة. ونجحت في إثبات أن النماذج التجميعية (Ensemble) – خاصة طريقة التكديس (Stacking) – تتفوق بشكل ملحوظ على النماذج الفردية في تحسين الدقة.

. دمج تقنيات المعالجة في الوقت الفعلي: من أبرز نقاط القوة في الدراسة هو دمجها لهندسة Kappa وإطار عمل Apache Spark لمعالجة البيانات في الوقت الفعلي. هذا النهج يعزز من قابلية تطبيق الحل المقترح في بيئة حية، حيث أن كشف الهجمات الفوري أمر بالغ الأهمية لسلامة المركبة.

٢. جوانب الضعف ومقترحات التحسين

على الرغم من نقاط القوة، توجد بعض الجوانب التي يمكن تحسينها لتعزيز القيمة العلمية والعملية للدراسة.

. التعامل مع مشكلة زمن التشغيل (Run-time):

◦ **النقد:** أشارت الدراسة إلى أن النماذج التجميعية، خاصةً التكديس (Stacking)، استغرقت زمن تشغيل أطول، يصل إلى "عشرات الثواني". ومع ذلك، اعتبرت الدراسة هذا التأخير "جديرًا بالاهتمام لتحقيق دقة أفضل". بالنسبة لنظام كشف تسلل في شبكة مركبة حساسة، فإن تأخيرًا بهذا الحجم يمكن أن يكون حرجًا ويهدد سلامة السائق والركاب.

◦ **مقترح التحسين:** كان من الأفضل أن تتناول الدراسة هذا التبادل بين الدقة والزمن بشكل أعمق. يمكن للباحث أن يقترح حلولًا لتقليل زمن الاستجابة، مثل استخدام أجهزة معالجة متخصصة (على سبيل المثال، وحدات المعالجة الرسومية GPU) أو تحسين الخوارزميات لتقليل التعقيد الحسابي.

٢. جوانب الضعف ومقترحات التحسين

. نطاق الهجمات المدروسة:

- النقد: ركزت الدراسة على أربعة أنواع من الهجمات وهي: DoS، Fuzzing، Replay، و Spoofing. هذه الهجمات شائعة، ولكن عالم الأمن السيبراني يتطور بسرعة.
- مقترح التحسين: يمكن للدراسة أن تتوسع في المستقبل لتشمل أنواعًا أخرى من الهجمات الأكثر تعقيدًا أو غير المعروفة (zero-day attacks)، والتي قد لا يتمكن النموذج الحالي من كشفها بسهولة. كما يمكن للباحث استكشاف قدرة النموذج على التكيف مع الهجمات المتغيرة باستمرار.

٢. جوانب الضعف ومقترحات التحسين

. غياب التطبيق العملي على بيئة حقيقية (Hardware-in-the-Loop):

◦ **النقد:** الدراسة هي عبارة عن "مخطط (scheme)" نظري يعتمد على تحليل البيانات المحفوظة من مجموعة بيانات عامة. لا يوجد أي ذكر لتطبيق عملي للنموذج على شبكة CAN حقيقية أو في بيئة محاكاة واقعية.

◦ **مقترح التحسين:** يمكن أن يكون هذا الجانب بمثابة مسار رئيسي لأبحاث مستقبلية. يجب على الباحث أن يوصي بضرورة اختبار المخطط المقترح على منصة مادية أو في بيئة محاكاة واقعية، لتقييم أدائه في ظروف العالم الحقيقي، وهو ما يعزز القيمة التطبيقية للدراسة بشكل كبير.

٢. جوانب الضعف ومقترحات التحسين

. التكرار في المحتوى:

النقد: يوجد بعض التكرار في الأفكار والجمل عبر فصول مختلفة من الرسالة، خاصة في وصف المنهجيات ونتائج النماذج.

مقترح التحسين: يُنصح بمراجعة النص لدمج الأفكار المتشابهة في أقسام واحدة، مما يجعل الرسالة أكثر انسيابية وتركيزاً. يمكن توحيد شرح المنهجية في قسم واحد شامل بدلاً من تكرارها في كل فصل من فصول النتائج.

٣. رؤية للتطوير المستقبلي

لتحويل هذه الدراسة من عمل أكاديمي قيم إلى إنجاز عملي مؤثر، يمكن للباحث أن يركز على مسارين رئيسيين:

التحقق العملي والواقعي:

- تطوير نموذج أولي (prototype) للمخطط المقترح وتطبيقه على منصة اختبار حقيقية لشبكة CAN في مركبة.
- قياس الأداء بدقة في ظروف التشغيل الواقعية، مع التركيز على زمن الاستجابة (Latency)، وليس فقط على الدقة.
- التحقيق في مدى قدرة النموذج على التعامل مع الضوضاء والبيانات غير المتوقعة في بيئة حية.

توسيع النطاق والتحديات:

- استكشاف تقنيات تعلم آلي متقدمة أخرى، مثل التعلم شبه الإشرافي (Semi-supervised Learning) أو التعلم المعزز (Reinforcement Learning)، التي قد تكون أكثر فعالية في كشف الهجمات الجديدة التي لا تحتوي على بيانات مصنفة.
- توسيع نطاق البحث ليشمل بروتوكولات اتصال أخرى في المركبات مثل FlexRay وAutomotive Ethernet، حيث أن الهجمات السيبرانية قد تستهدف نقاط ضعف متعددة.

خاتمة

في الختام، تُعد هذه الدراسة مساهمة علمية مهمة في مجال الأمن السيبراني للمركبات. فقد نجحت في بناء أساس نظري ومنهجي قوي، وقدمت نتائج واعدة فيما يتعلق بدقة نماذج التعلم التجميعي. ومع ذلك، فإن القيمة الحقيقية لهذا البحث تكمن في قدرته على التحول من كونه دراسة نظرية إلى حل عملي قابل للتطبيق. من خلال معالجة التحديات المتعلقة بالوقت، وتوسيع نطاق الهجمات، وإجراء اختبارات على أرض الواقع، يمكن للباحث أن يضع حجر الأساس لجيل جديد من أنظمة كشف التسلل التي تضمن سلامة وأمان المركبات المستقبلية.





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

