مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (٤) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (4) 2025

خوارزمية الثقة المعتمدة على المتوسط الموزون للتحديد سلوك العربات في VANET

أ.د. غسان محمد *

د. ناجي ابراهيم محمد **

م. ازدهار شفيق شاليش ***

(تاريخ الإيداع ٢٠٢٤/١٠/٢٧ . قُبِل للنشر في ٢٠٢٥/٤/٢٨)

□ ملخّص □

تعد شبكات VANET حلاً حيوياً لتعزيز سلامة السائقين، حيث تساهم في توعية السائقين بمعالم الطريق وتوجيههم للالتزام بها. ومع ذلك، يمكن أن تشكل هذه الشبكات تهديدًا على الأمان عند استغلالها لأغراض ضارة، مثل التنصت على السائقين أو تعقبهم، أو التلاعب بالرسائل وإعادة إرسالها مما قد يؤدي إلى حوادث جسيمة تصل إلى حد الوفاة. للتصدي لهذه التهديدات، تقترح الدراسة إجراء تحليل عميق لخوارزميات الكشف عن سوء السلوك في شبكات VANET. يتم ذلك من خلال اختبارات دقيقة للتحقق من صحة الرسائل المتبادلة في الشبكة. تم اقتراح خوارزمية تعتمد على المتوسط الموزون في حساب الثقة في تحديد هل سلوك العربة سلوك جيد أم لا .حيث تم دراسة الخوارزمية المقترحة في حالة كثافة الهجوم العالية و المنخفضة وبحالة كثافة المرورية العالية و العادية ،بينت النتائج أن الدقة Precision عالي بنسبة ٥١% و F1-score بنسبة ٥٠% عند تطبيقها في كثافة المرورية العالية بكثافة مهاجم عالية.

الكلمات المفتاحية:

الكشف عن سوء السلوك، شبكات VANETs، هجوم، اختبارات، رسائل المنارة .

*أستاذ دكتور، كلية هندسة تكنولوجيا المعلومات والاتصالات، جامعة طرطوس، طرطوس، سورية.

**أستاذ مساعد كلية هندسة تكنولوجيا المعلومات والاتصالات، جامعة طرطوس، طرطوس، سورية.

***طالبة دراسات عليا(دكتوراه)، قسم تكنولوجيا الاتصالات، كلية هندسة تكنولوجيا المعلومات والاتصالات، جامعة طرطوس، طرطوس، سورية.

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (٤) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (4) 2025

Weighted Average-Based Trust Algorithm for Determining Vehicle Behavior in VANET

*** Prof. Dr. Ghassan Mohammed**
**** Dr. Naji Ibrahim Mohammad**
***** Eng. Izdihar Chafick Chalich**

(Received 27/10/2024 . Accepted 28/4/2025)

□ ABSTRACT □

VANET networks represent a vital solution for enhancing driver safety by raising awareness about road landmarks and guiding drivers to adhere to them. However, these networks can pose a security threat when exploited for malicious purposes, such as eavesdropping on drivers, tracking them, or manipulating and retransmitting messages, potentially leading to severe accidents, including fatalities. To counter these threats, the study proposes a comprehensive analysis of misbehavior detection algorithms in VANET networks. This involves rigorous testing to validate the exchanged messages within the network. A weighted average-based algorithm is proposed to calculate trust in determining whether a vehicle's behavior is legitimate or not. The proposed algorithm was evaluated under scenarios of high and low attack density, as well as under high and normal traffic density. The results showed that the Precision was high at 51%, and the F1-score was 50% when applied in high traffic density with a high attacker density.

Key Words: Misbehavior detection، VANETs، attack، checks، detectors, beacon messages.

***Professor, Faculty of Information and Communication Technology Engineering, Tartous University, Tartous, Syria.**

1- مقدّمة

تهدف شبكاتVANET (Vehicular Ad-Hoc Network) إلى تعزيز السلامة على الطرق من خلال تقليل الحوادث المرورية الناتجة عن السرعات الزائدة أو عدم إدراك السائق للتضاريس المحيطة بالطريق. لتحقيق ذلك، تم تطوير نظام يسمح بتبادل الرسائل بين العربات، بحيث تحتوي هذه الرسائل على معلومات حول حالة الطريق، بالإضافة إلى معرف خاص بالعربة المرسلة. ومع أن هذه الرسائل تُرسل عبر شبكات لاسلكية، فهي عرضة لنوعين من الهجمات:

١. الهجوم الخارجيExternal attack : يتمثل في اعتراض رسائل Beacons بهدف تعقب العربات ومتابعة مسارها من لحظة الانطلاق حتى الوصول إلى الوجهة. وقد دفع هذا النوع من التهديد الباحثين إلى تطوير أنظمة لحماية الخصوصية تهدف لحماية السائقين من التتبع من خلال تغيير الأسماء المستعارة للمركبات بشكل مدروس.

٢. الهجوم الداخليInternal attack : يعد هذا النوع الأكثر خطورة مقارنةً بالتنصت، إذ يقوم المهاجم بتعديل محتوى رسائل Beacons، مما قد يؤدي إلى اتخاذ السائق قرارات غير مناسبة وفقًا للمعلومات الخاطئة، مما يزيد من احتمالية الحوادث التي تهدد سلامة السائقين، الركاب، والمشاة.

لتحقيق فعالية شبكة VANET، يجب ضمان تلبية متطلبات الأمن الأساسية، وأهمها المصادقة (Authentication)، وسلامة البيانات (Data Integrity)، والحفاظ على السرية (Confidentiality)، لضمان استمرارها في تحقيق هدفها الأساسي. وعلى الرغم من تزويد العربات عند تسجيلها الأول بمجموعة من الأسماء المستعارة والشهادات الرقمية، مع إمكانية استخدام التشفير، إلا أن هذه التدابير أصبحت غير كافية، إذ لا يزال بإمكان المهاجم استخدام معلوماته الخاصة لشن هجوم معين ، أو أن يحتفظ بمعلومات قادمة من عربة مجاورة لاستخدامها لاحقا لشن هجوم معين ، لتجنب ذلك، تم اقتراح ان يتم انشاء معرف خاص بكل RSU (Road side unit)، وتسجل العربات معرفات RSU لديها ، عندما تصل إلى RSU جديد ، فانه يقوم باختبار سلسلة المعرفات لتأكد من أن رسالة سليمة ، ففي حال كانت السلسلة صحيحة تكون الرسالة شرعية وإلا تعتبر رسالة سيئة السلوك.

لكن هذه الدراسة تفترض أن الهجوم ممكن أن يتم من قبل العربات، لكن يستطيع المهاجم إذا استطاع الوصول الى بيانات RSU، من استغلالها وشن الهجوم باستخدام بياناتRSU، بالإضافة إلى إمكانية تعقب العربات وبالتالي الإخلاء بالخصوصية[1] .

تم استخدام بارامتر السرعة لتحديد هل يوجد هجوم أو لا، وذلك من خلال قيام العربة المستقبلة باختبار الرسالة التي استقبلتها، في حال كانت العربة المرسلة ليست موجودة ضمن قائمة الجوار لديها، فستقوم بإضافتها، أما في حال كانت العربة المرسلة موجودة ضمن القائمة، هنا تقوم بحساب الفرق بين السرعة الحقيقية للعربة والسرعة المقدرة لها، في حال كان الفرق أكبر من عتبة الكشف يتم تشغيل مؤقت زمني وبث رسالة

**Assistant Professor, Faculty of Information and Communication Technology Engineering, Tartous University, Tartous, Syria.
***Postgraduate Student, Department of Communication Technology, Faculty of Information and Communication Technology Engineering, Tartous University, Tartous, Syria

beacons للجوار لتأكيد وجود هجوم، في حال وصول رسالة تأكيد الهجوم يتم اتخاذ التدابير المضادة لإيقاف الهجوم. لكن هذه الدراسة تعاني من أن المهاجم يستطيع أن يستخدم أسماء مستعارة لتوليد عربات وهمية [2].

بما أن الهجوم يستغل احدى بارامتر رسالة beacon، فقد وجد الباحثون أنه من الضروري إجراء اختبار على كل بارامتر في الرسالة. تم تطوير اختبارات المعقولية التي تحدد ما إذا كانت الرسالة المستقبلة معقولة أم لا، بالإضافة إلى اختبارات التطابق التي تقارن البيانات بين رسائل الـ beacon المستقبلة والرسائل السابقة.

اقترحت بعض الدراسات أيضًا أن يتم الكشف عن سوء السلوك في وحدات RSU نظرًا لما تمتلكه من قدرات معالجة تتفوق على قدرات العربات. عندما تستقبل وحدة الـ RSU رسالة من عربة ضمن نطاق تغطيتها، تتصل بقاعدة بيانات مشتركة بين جميع وحدات الـ RSU لاسترداد آخر رسالة beacon أرسلتها العربة. بعد ذلك، تقوم بدمج الرسالة المستقبلة من العربة مع الرسالة الواردة من قاعدة البيانات المشتركة، ثم تطبق عليها نماذج التعلم الآلي لتحديد ما إذا كانت الرسالة صحيحة أو تحتوي على معلومات مزيفة. في حال اكتشفت وحدة الـ RSU أن العربة تصدر سلوكاً مشبوهاً، تقوم بإبلاغ العربات ووحدات الـ RSU الأخرى ضمن نطاق تغطيتها، بهدف تسجيل ملاحظة على العربة في سجلاتهم. تفترض هذه الخوارزمية أن وحدات الـ RSU آمنة، ولكن إذا تمكن المهاجم من الوصول إلى وحدات الـ RSU واستخدام شهاداتها لإرسال رسائل مزيفة، فإن ذلك قد يزيد من خطورة الضرر. بالإضافة إلى ذلك، فإن الخوارزمية قد تخرق شرط الخصوصية لأنها تستدعي الرسالة المرسلة باستخدام المعرف الأساسي للعربة [3].

يعتبر هجوم Sybilمن الهجومات الشائعة والتي يكون ضررها على الشبكة كبيرة، وذلك لأنه يعتمد ارسال رسائل بأسماء مستعارة مختلفة إلى العقد الأخرى الموجودة في الشبكة، حيث تسمى العقد التي ترسل الرسائل المزيفة بعقد الهجوم، بينما العقد التي تستقبل هذه الرسائل المزيفة تسمى عقد Sybil، حيث يمكن باستخدام هذا الهجوم، إنشاء ازدحام مروري مزيف، بهدف إجبار العربات الشرعية على تغيير مسارها. وجدت الدراسة أنه بحال وجود هجوم Sybil، فإن بارامتر نسبة إيصال المحتوى ومعدل اسقاط الرزم تتأثر بحسب قوة الهجوم، كلما كان الهجوم قوي كلما انخفضت نسبة توصيل المحتوى وزاد معدل إسقاط الرزم [4]، لكن لم توضح الدراسة البارامترات التي اعتمدتها لتنفيذ الهجوم.

معظم الدراسات اعتمدت على استخدام التعلم الألي في الكشف عن سوء السلوك دون ذكر الخوارزمية الأساسية التي قامت بتوليدdataset، بالإضافة إلى أن بعضهم اعتمد على دراسة هجوم محدد دون غيره.

بالإضافة إلى الهجمات، قد تُرسل العربات معلومات خاطئة عن غير قصد بسبب خلل في حساسات العربة. وقد دفعت هذه المخاطر الباحثين إلى دراسة وتطوير طرق فعالة للكشف عن السلوكيات غير السليمة الناتجة عن الهجمات الداخلية أو الأخطاء التقنية في الحساسات، بهدف تحسين سلامة النظام بشكل عام.

2-هدف البحث

هدف البحث إلى الكشف عن سوء السلوك الناتج عن الهجومات التي يتم تطبيقها على شبكات VANETعن طريق مهاجم خارجي يستغل العربات الشرعية لشن الهجوم، أو عن طريق معلومات خاطئة ناتجة عن حساسات معيبة لسبب ما.

3- طرائق البحث و مواده

أُجريت المحاكاة باستخدام VEINSوهو عبارة عن إطار محاكاة اتصال بين العربات يعتمد على نموذج محاكاة ثنائي الاتجاه وله دخلين هما OMNET++ برنامج محاكاة الشبكة القائم على الحدث (Objective Modular Network Testbed in C++) وSUMO (Simulation of Urban Mobility) برنامج محاكاة حركة المرور على الطريق وسبب اختيار VEINSهو قدرته على محاكاة طبقات الشبكة الكاملة 802.11P، IEEE 1609.4 DSRC / WAVE.

٣-1 نموذج المهاجم

مهاجم داخلي له إمكانية استغلال شهاداته واسمائه المستعارة لتنفيذ هجوم معين بهدف تحقيق غرض معين، أو يمكن أن يستغل عربة شرعية لتنفيذ هجومه. يقوم هذا المهاجم بعدة هجمات ومنها [3] :

١- هجوم DOS: يعتمد ألية تنفيذه على زيادة تردد رسالة Beacon بحيث تمنع بقية العربات من الوصول إلى الشبكة.

٢- هجوم Disruptive: يحصل المهاجم على رسائل Beacons من العربات المجاورة له فيقوم بتسجيل هذه البيانات الواردة في رسائل Beacons لكي يستخدمها في ارسال رسائله.

يعد هذا الهجوم خطير على اعتبار أن هذه الرسائل تكون خاطئة إلا أنها تكون صادرة عن عربات أصلية في البداية لذلك تبدو معقولة.

٣- هجوم Eventual Stop: تتصرف عربة المهاجم بشكل طبيعي لفترة زمنية معينة ثم تصبح ثبت رسالة متضمنة سرعتها مساوية للصفر وبالتالي تحاكي التوقف النهائي الطبيعي للعربة.

٤- هجوم Traffic Congestion Sybil:

يخزن المهاجم الأسماء المستعارة الواردة في رسائل Beacons التي استقبلها من الجيران، ثم يقوم بإجراء الحسابات لأنشاء العربات الوهمية بحيث يكون موقع وسرعة واتجاه العربات الوهمية متناسبة وفقاً لبيانات العربة المستهدفة. ثم يعطي اسم مستعار لكل عربة وهمية ويزيد من تردد رسائل beacons.

بالإضافة إلى ارسال رسائل beaconsمتضمنة معلومات حركية خاطئة قد تكون ناتجة عن خطأ ناتج عن حساسات العربة ذاتها أو قد يقوم بها المهاجم بشكل متعمد[3] :

٥- Fixed Position: تقوم العربة \المهاجم ببث موقعاً خاطئاً بشكل دائم.

٦- Fixed Position Offset: تبث العربة \المهاجم موقعه الحقيقي مع إزاحة ثابتة.

٧- Random Position: يبث موقعاً عشوائياً يكون بين قيم صغرى وقيم كبرى محددة سابقا في المحاكاة.

٨- Random Position Offset: يبث موقعاً حقيقاً مع إزاحة عشوائية.

٩- :Fixed Speed تبث العربة \المهاجم سرعة ثابتاً بشكل دائم.

١٠- Fixed Speed Offset: تبث العربة \المهاجم سرعة حقيقة مع إزاحة ثابتة.

١٢- Random Speed: تبث العربة \المهاجم سرعة عشوائية.

١٣- Random Speed Offset: تبث سرعتها الحقيقية مع إزاحة عشوائية.

2-3 -الخوارزمية الثقة التقليدية (Trust Algorithm)

خوارزمية الثقة التقليدية (Trust Algorithm) تعتمد على أصغر قيمة للفحوصات في حساب مستوى الثقة(Trust level) لدى العربة لتحديد هل العربة شرعية أم عربة مهاجم كما هو موضح بالمعادلة (١) ، هذا الأمر قد يجعل الخوارزمية تحدد سلوك العربة وفقاً لهذا الفحص الواحد الأصغر بغض النظر عن قيمة بقية الفحوصات التي تلعب دوراً مهما في الكشف.

$$\textbf{Trust level} = -\frac{\mathbf{e}^{(10(1-C_{min})} + \mathbf{1}}{\mathbf{2 * 10^4}} \qquad (\mathbf{1})$$

حيث إن C_{min} تمثل قيمة أصغر فحص من بين مجموعة الفحوصات التي تجريها العربة.

٣-3- الخوارزمية المقترحة (Proposed Algorithm)

تم اقتراح خوارزمية تفرض على العربة المستقبلة فحص كل رسالة Beacons ورادة لها وذلك من خلال تطبيق مجموعة من الفحوصات، ثم تطبيق المتوسط الموزون لكل هجوم ، بحيث يتم إعطاء أوزان مختلفة لكل فحص وذلك حسب نوع الهجوم الذي تم اكتشافه . تعطى علاقة المتوسط الموزون :

$$\textbf{Weight Average} = \frac{\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{w_i} * \mathbf{x_i}}{\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{w_i}} \qquad (\mathbf{2})$$

حيث إن x_i : قيمة الفحص i.

w_i : وزن الفحص i.

ثم يتم حساب مستوى الثقة وفقاً للخوارزمية المقترحة بالمعادلة (٣) :

$$\textbf{Trust level} = -\frac{\mathbf{e}^{(10(1-\textbf{Weight Average})} + \mathbf{1}}{\mathbf{2 * 10^4}} \qquad (\mathbf{3})$$

ثم يتم مقارنة قيمة مستوى الثقة مع عتبة محددة مسبقاً، في حال كانت قيمة مستوى الثقة أقل من ٠,٥، يتم الإبلاغ عن العربة على إنها عربة مهاجم و تسلك سلوك سيء في الشبكة.

تخزن العربات المستقبلة لديها قيمة مستوى الثقة لكل رسالةBeacons ترد إليها ، ففي حال كانت قيمة مستوى الثقة أعلى من 0.5، يتم زيادة مستوى الثقة بمقدار ٠,١ على أن لا تتجاوز قيمة مستوى الثقة ١.

تمت دراسة المقارنة بين الخوارزمية المقترحة و خوارزمية الثقة التقليدية التي كانت تعتمد على أصغر قيمة للفحص لحساب مستوى الثقة الذي يحدد هل سلوك العربة سليم أم لا.

٣-4 اختبارات المعقولية والتطابق(Plausibility and Consistency checks)

تجرى فحوصات المعقولية على كل رسالةbeacon للتأكد من معقولية موقعها وإنها واقعة ضمن مجال تغطية العربة المستقبلة وسرعتها وترددها.

بينما تجرى فحوصات التطابق بمقارنة الرسالة beacon الواردة في اللحظة t مع رسالة beacon الواردة في اللحظة t-1 لنفس المرسل للتأكد من أن العربة قطعت مسافة بسرعة معينة و بتسارع أو تباطؤ معين ضمن الحدود المعقولة .

تمت إضافة فحص للاسم المستعار من خلال تطبيق تابع Hash عليه ، وذلك لضمان إنه لا يوجد لدينا عربتين لهما نفس الاسم المستعار [2].

٣-5- مقاييس الكشف[3]

٣-5-١ مصفوفة الارتباك Confusion Matrix :

تصف مصفوفة الارتباك الحالات التي تم اكتشافها بشكل صحيح والحالات الخاطئة كما هو موضح في الجدول (١).

الجدول (١) مصفوفة الارتباك

رسالة قادمة من عربة مهاجم	رسالة قادمة من عربة شرعية	خوارزمية الكشف
TP	FP	تم الكشف
FN	TN	لم يتم الكشف

حيث إن TP(True Positive): تمثل عدد الحالات التي وردت من عربة مهاجم واستطاعت الخوارزمية كشفها.

FP(False Positive): هنا قامت الخوارزمية بتأكيد وجود سلوك سيء الا إنه في الحقيقة هو سلوك جيد أي انذار كاذب أي تم تصنيف عربة شرعية كمهاجم.

FN(False Negative) :الخوارزمية فشلت في التعرف على سلوك المهاجم، مما يعني أنه لم يتم الكشف عن الهجوم .

TN (True Negative) : نجحت الخوارزمية في تصنيف العربة على أنها شرعية بشكل صحيح.

٣-٤-٢ الدقة Accuracy:

هي معدل الاتفاق الإيجابي، الذي يشير الى نسبة اكتشاف الحقيقي في النظام، تعطى علاقته:

$$\mathbf{Accuracy} = \frac{\mathbf{TP} + \mathbf{TN}}{\mathbf{TP} + \mathbf{FP} + \mathbf{TN} + \mathbf{FN}} \quad (4)$$

٣-٤-٣ الدقة الإيجابية (الموثوقية) Precision:

تقيس نسبة الرسائل التي تم وضع علامة عليها بشكل صحيح على إنها تعمل بشكل سيئة من بين جميع الرسائل التي تم وضع علامة عليها. تشير Precision إلى قدرة الخوارزميات على التمييز بين العقد غير صحيحة والعقد الشرعية.

$$\mathbf{Precision} = \frac{\mathbf{TP}}{\mathbf{TP} + \mathbf{FP}} \quad (5)$$

٣-٤- ٤ الاسترجاع Recall:

يقيس نسبة الرسائل التي تم تحديدها بشكل صحيح والتي تسيء السلوك من بين جميع الرسائل سيئة السلوك المستقبلة.

$$\mathbf{Recall} = \frac{\mathbf{TP}}{\mathbf{TP} + \mathbf{FN}} \quad (6)$$

٣-٤-٥ معيار F1-score

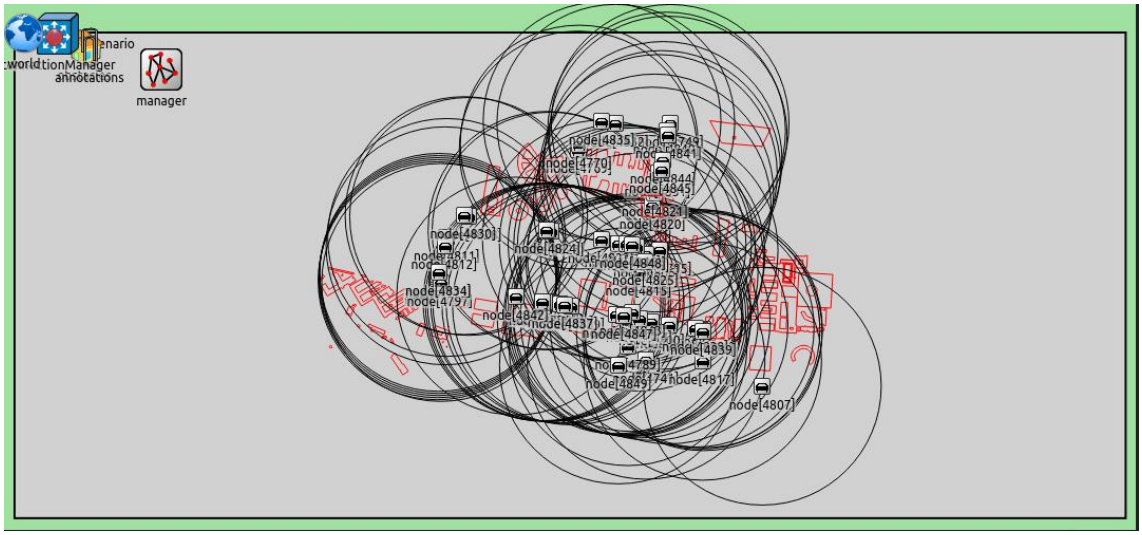
هو المتوسط التوافقي للRecall، Precision ، يمكن استخدامه كمقياس واحد لتقييم أداء النظام، حيث تعطى نفس الأهمية لـ Recall، Precision .

$$\mathbf{F1 - Score} = 2 * \frac{\mathbf{Recall} * \mathbf{Precision}}{\mathbf{Recall} + \mathbf{Precision}} \quad (7)$$

٣-٥ المحاكاة والمناقشة

تم إجراء المحاكاة على مدينة باريس الفرنسية باستخدام SUMO&OMNET لتوفر بيانات الخريطة وبيانات الحركة المطلوبة للمحاكاة [12]كما هو موضح في الشكل (١) و باستخدام بارامترات المحاكاة الواردة في الجدول (2) .

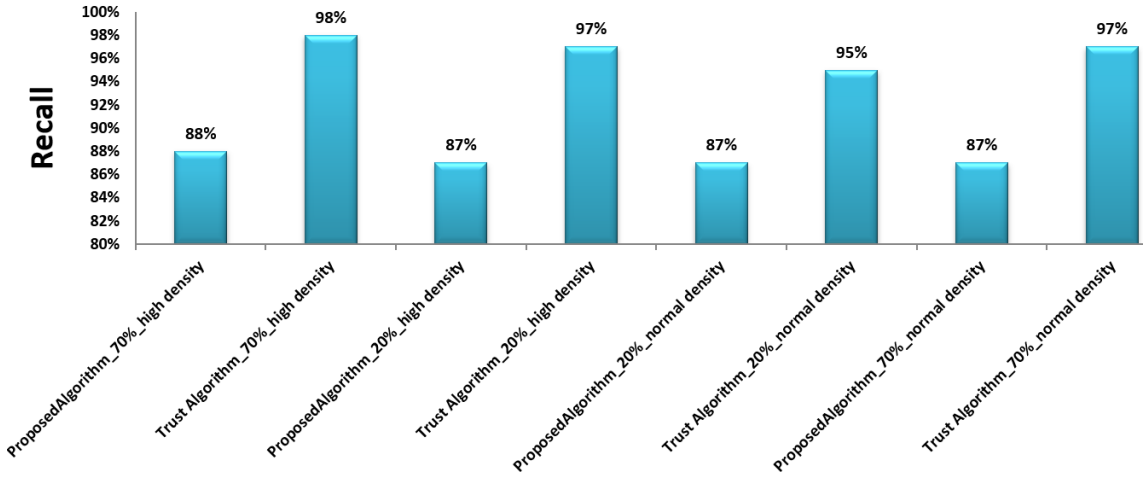
تم تطبيق عدة سيناريوهات تحاكي كثافات متعددة للهجوم مع دراسة حالة كثافة المرورية بحالة العادية normal density والكثافة المرورية العاليةhigh density .



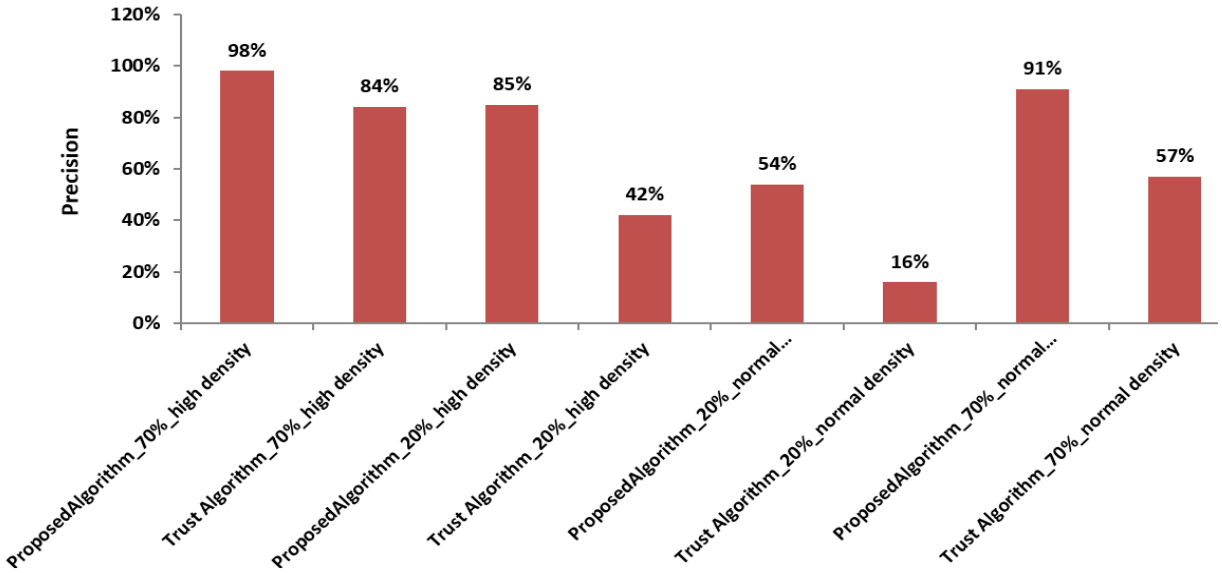
الشكل (١) المحاكاة في OMNET++

الجدول (2) بارامترات المحاكاة

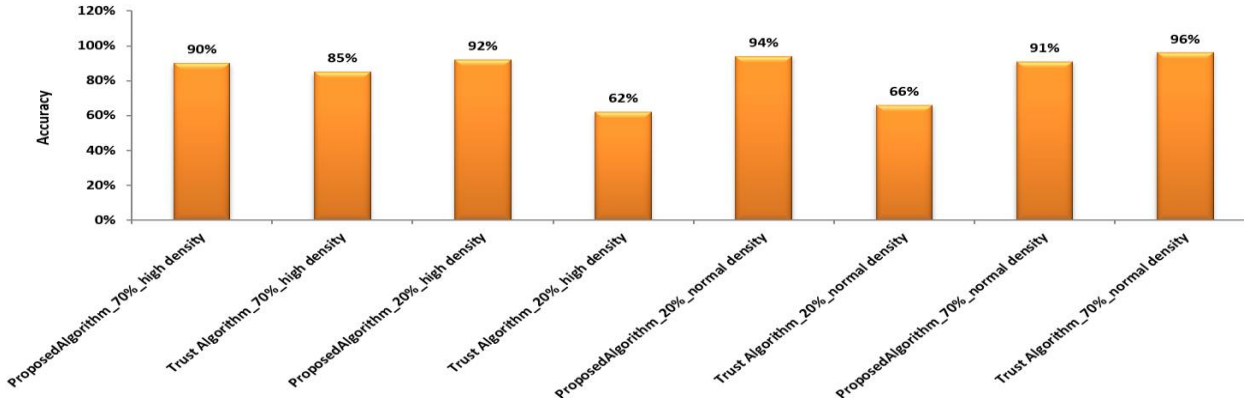
Module	Parameter	Default Value
Veins	Transmission Power	**20mw**
	Bit Rate	**6Mbps**
	Packet Header length	**80bit**
	Beacon Payload length	**100 byte**
	Beacon rate	**1 HZ**
Attacks Parameters	Attack Probability	**20%,70%**



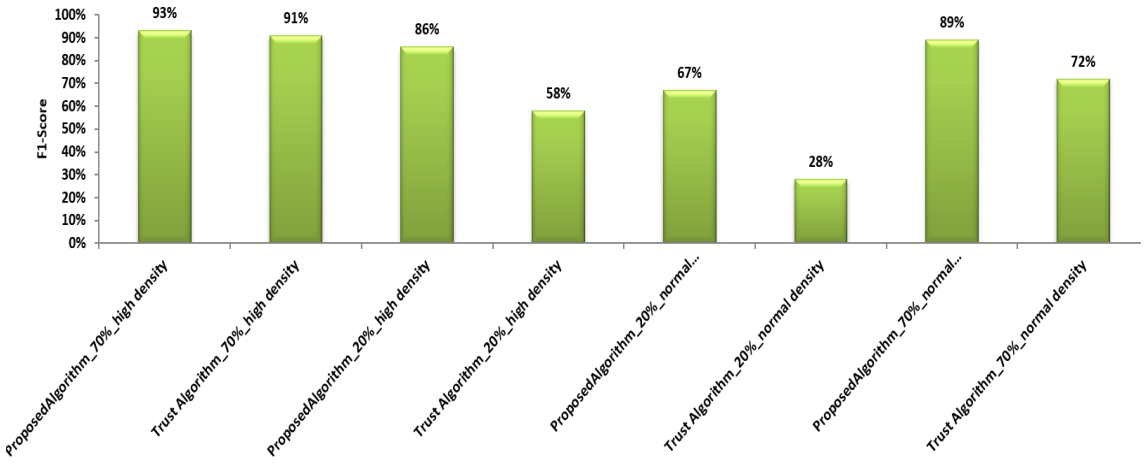
الشكل (2) مقارنة Recall للخوارزمية المقترحة و الخوارزمية الثقة التقليدية بحالة عدة كثافات للهجوم وبحالة كثافة المرور العادية و العالية



الشكل (3) مقارنة Precision للخوارزمية المقترحة و الخوارزمية الثقة التقليدية بحالة عدة كثافات للهجوم وبحالة كثافة المرور العادية و العالية



الشكل (4) مقارنة Accuracy للخوارزمية المقترحة و الخوارزمية الثقة التقليدية بحالة عدة كثافات للهجوم وبحالة كثافة المرور العادية و العالية



الشكل (5) مقارنة F1-Score للخوارزمية المقترحة و الخوارزمية الثقة التقليدية بحالة عدة كثافات للهجوم وبحالة كثافة المرور العادية و العالية

أعطت Trust Algorithm بحالة كثافة الهجوم 70% وبكثافة مرورية عالية أعلى قيمة Recall كما في الشكل (2) والسبب في ذلك يعود إلى أن الخوارزمية تعتمد في الأساس على ادخال أقل قيمة للفحوصات بغض النظر عن نوع الهجوم المكتشف الى معادلة مستوى الثقة، مقارنة مع خوارزمية المقترحة التي تعتمد على إعطاء أوزان للفحوصات حسب الهجوم المكتشف ومن ثم إدخال نتيجة المتوسط الموزون إلى معادلة مستوى الثقة .

عندما تكون Recall عالية ، يعني أن FN منخفض (عدد الحالات التي صنفتها الخوارزمية على إنها سلبية لكنها كانت ايجابية) و TPعالي (عدد الحالات التي صنفتها الخوارزمية على إنها حالات إيجابية كانت بالفعل ايجابية).

تزداد قيمة Recall عند حالة كثافة مهاجم عالية وتنخفض بحالة كثافة المهاجم المنخفضة وذلك لانخفاض عدد الحالات المدروسة .

أثبت الخوارزمية المقترحة Proposed Algorithm بحالة الكثافة المرورية العالية وكثافة المهاجم العالية ٧٠% إنها لديها القدرة على تصنيف الحالات الإيجابية بشكل صحيح حيث أعطت أعلى قيمة Precision كما في الشكل (٣)مقارنة ببقية السيناريوهات ويعود ذلك إلى إعطاء وزن لكل فحص وفقاً للهجوم المكتشف .

تتأثر قيمةPrecision بكثافة الهجوم ، حيث تزداد عند زيادتها والعكس صحيح.

لكن دهورت قيمةPrecision عند تطبيق الخوارزمية التقليدية Trust Algorithm وخاصة عند تطبيقها مع الكثافة المرورية العادية أو العالية مع كثافة مهاجم منخفضة .

يمثل المقياسF1-Score توازنا بينPrecisionو Recall، حيث استطاعت الخوارزمية المقترحة بحالة الكثافة المرورية العالية و بكثافة هجوم عاليةمن تحقيق أعلى قيمة F1-score.

أيضا تتأثر قيمةF1-score بكثافة الهجوم ،حيث تزداد مع زيادتها والعكس صحيح.

أبدت خوارزمية التقليديةTrust Algorithm تدهورا واضحاً قي قيمة F1-Score وخاصة عند تطبيقها بحالة الكثافة العادية و كثافة مهاجم منخفضة ٢٠% كما في الشكل (٥).

أثبت الخوارزميةTrust Algorithm فعاليتها في حال تطبيقها في سيناريو كثافة مرورية العادية و كثافة مهاجم عالية ٧٠% من ناحيةAccuracy كما في الشكل (٤).

لكنها تعتبر غير جيدة عند تطبيقها في سيناريو الكثافة العالية بحالة كثافة هجوم منخفضة.

٤- الاستنتاجات والتوصيات

تمت محاكاة خوارزمية الثقةTrust Algorithm التقليدية المعتمدة على إيجاد أقل قيمة للفحوصات وإدخالها الى معادلة مستوى الثقة ، التي يتم مقارنة النتيجة مع عتبة محددة مسبقاً ، لم تأخذ هذه الخوارزمية نوع الهجوم المكتشف وإنما اعتمدت على أقل قيمة للفحص في تحديد هل هذا سلوك صادر عن عربة شرعية أم عربة مهاجم، على خلاف الخوارزمية المقترحة التي اعتمدت بشكل أساسي على نوع الهجوم المكتشف في إعطاء اوزان مختلفة للفحوصات وفقاً للهجوم المكتشف ومن ثم حساب المتوسط الموزون وإدخال قيمة المتوسط الموزون الى معادلة الثقة التي تحدد عند مقارنتها مع عتبة محددة مسبقا هل العربة شرعية أم لا .

درست الخوارزميتين بعدة حالات : بحالة الكثافة المرورية العادية normal التي تمثل الفترة الممتدة بين ٩صباحا الى ساعة ١ ظهراً ، لكن الكثافة المرور العالية تحدث في الصباح وأثناء خروج الموظفين من أماكن عملهم يمكن أن يحدث ازدحام مروري .

تم أخذ بعين الاعتبار كثافتين للهجوم : كثافة هجوم عالية :٧٠% أي تم تطبيق هجمات على الشبكة بحدود٧٠% مقارنة مع كثافة الهجوم المنخفضة ٢٠% .

تم استنتاج أن :

الخوارزمية التقليدية Trust بحالة كثافة المرورية العادية مع كثافة هجوم عالية (Trust_Algorithm_70%_normal)حققت أعلى قيمة Accuracy بنسبة ٩٦% .

أيضا استطاعت الخوارزمية التقليدية تحقيق Recall عالي بنسبة ٩٧% لكن عند تطبيقها في سيناريو كثافة المرورية العالية (Trust Algorithm_70%_High).

استطاعت الخوارزمية المقترحةProposed Algorithm عند تطبيقها في سيناريو الكثافة المرورية العالية و بحالة كثافة هجوم عالية ٧٠% من تحقيق أعلى قيمة F1score بنسبة ٩٣%و Precision بنسبة 98%.

من أجل الحصول على أعلى نسبة في التصنيف الصحيح ، يمكن أن يتم إدخال النتائج الفحوصات إلى مرشحات تعمل على إزالة الإنذارات الكاذبة و بالتالي زيادة دقة الكشف .

٥- المراجع

[1] Hamdan, S., Hudaib, A., & Awajan, A. (2021). Detecting Sybil attacks in vehicular ad hoc networks. International Journal of Parallel, Emergent and Distributed Systems, 36(2), 69-79.

[2] Zhou, T., Choudhury, R. R., Ning, P., & Chakrabarty, K. (2007, August). Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. In 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous) (pp. 1-8). IEEE.

[3] Sharma, A., & Jaekel, A. (2021). Machine learning based misbehaviour detection in VANET using consecutive BSM approach. IEEE Open Journal of Vehicular Technology, 3, 1-14.

[4] Grover, J., Laxmi, V., & Gaur, M. S. (2012). Misbehavior detection based on ensemble learning in vanet. In Advanced Computing, Networking and Security: International Conference, ADCONS 2011, Surathkal, India, December 16-18, 2011, Revised Selected Papers (pp. 602-611). Springer Berlin Heidelberg.

[5] Sonker, A., & Gupta, R. K. (2021). A new procedure for misbehavior detection in vehicular ad-hoc networks using machine learning. International Journal of Electrical & Computer Engineering (2088-8708), 11(3).

[6] Khot, A., & Dave, M. (2021). Position falsification misbehavior detection in vanets. In Mobile Radio Communications and 5G Networks: Proceedings of MRCN 2020 (pp. 487-499). Springer Singapore.

[7] Singh, P. K., Gupta, S., Vashistha, R., Nandi, S. K., & Nandi, S. (2019). Machine learning based approach to detect position falsification attack in VANETs. In Security and Privacy: Second ISEA International Conference, ISEA-ISAP 2018, Jaipur, India, January, 9–11, 2019, Revised Selected Papers 2 (pp. 166-178). Springer Singapore.

[8] Mangla, C., Rani, S., & Herencsar, N. (2023). A misbehavior detection framework for cooperative intelligent transport systems. ISA transactions, 132, 52-60.

[9] Van Der Heijden, R. W., Dietzel, S., Leinmüller, T., & Kargl, F. (2018). Survey on misbehavior detection in cooperative intelligent transportation systems. IEEE Communications Surveys & Tutorials, 21(1), 779-811.

[10] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. Vehicular Communications, 23, 100214.

[11] Hussain, R., Lee, J., & Zeadally, S. (2020). Trust in VANET: A survey of current solutions and future research opportunities. IEEE transactions on intelligent transportation systems, 22(5), 2553-2571.

[12] Codeca, L., Frank, R., & Engel, T. (2015, December). Luxembourg sumo traffic (lust) scenario: 24 hours of mobility for vehicular networking research. In 2015 ieee vehicular networking conference (vnc) (pp. 1-8). IEEE.