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

دراسة تأثير المجال الأعظمي المعقول للتغطية على أداء خوارزميات الكشف عن سوء السلوك في شبكات VANET

أ.د. غسان محمد *

د. ناجي ابراهيم محمد **

م. ازدهار شفيق شاليش ***

(تاريخ الإيداع ٢٠٢٥/٦/١٦ . قُبِل للنشر في ٢٠٢٥/٨/١٨)

□ ملخّص □

يُعد المجال الأعظمي المعقول للتغطية في شبكات العربات (VANETs) هو النطاق الذي تتمكن فيه العربات من تبادل رسائل beacons لتحذير السائقين من ظروف الطريق. ورغم أن توسيع هذا المجال يسمح باستقبال رسائل أكثر من عربات متعددة، إلا أنه لا يضمن موثوقية هذه الرسائل، مما قد يفتح الباب لهجمات خبيثة تؤثر على سلامة القيادة. كما يمثل مجال الظهور المفاجئ حالة تظهر فيها عربة بشكل مفاجئ داخل مجال عربة أخرى دون تبادل تدريجي للرسائل، مما يعزز فرص الهجوم أو التشويش. لمعالجة هذه التحديات، نقترح خوارزمية الثقة القائمة على متوسط الموزون للفحص(TrustWeightCheck) التي تعتمد على دمج الثقة مع أوزان ديناميكية للفحوصات، بحيث يُعزز وزن الفحص الفاشل ويُقلل وزن الفحص الناجح دون إهمال أي نتيجة. وقد تم تقييم أداء الخوارزمية ضمن قيمتين للمجال ٤٢٠م و٦٠٠م. أظهرت النتائج أن زيادة المجال تؤثر بشكل طفيف على أداء الكشف، من خلال ارتفاع بسيط في زمن الاكتشاف وانخفاض محدود في مقاييس F1–Score، إلا أن الخوارزمية المقترحة تفوقت من حيث سرعة الكشف، حيث حققت متوسط زمن اكتشاف بلغ ٠.١٣ ثانية، إلى جانب معدل F1–Score مرتفع بلغ ٥٨٪. وعلى الرغم من ارتفاع الانتروبيا في تحديد العربة المهاجمة نتيجة تغيّر الأسماء المستعارة لتقليل إمكانية التتبع، فقد أظهرت الخوارزمية توازناً جيداً في الاعتماد على جميع الفحوصات، مقارنة بخوارزميات تعتمد على معيار واحد أو ثقة الجوار أو على تنبؤات أولية بنوع الهجوم.

الكلمات المفتاحية: الكشف عن سوء السلوك، شبكات VANETs، هجوم، اختبارات، إنذارات كاذبة .

*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 (٩) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (9) 2025

Studying the Impact of the Maximum Plausible Coverage Range on the Performance of Misbehavior Detection Algorithms in VANETs

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

(Received 16/6/2025 . Accepted 18/8/2025)

□ ABSTRACT □

The maximum plausible coverage range in Vehicular Ad Hoc Networks (VANETs) is the distance within which vehicles can exchange beacon messages to warn drivers about road conditions. Although extending this range allows receiving messages from multiple vehicles, it does not guarantee the reliability of these messages, which may open the door to malicious attacks that affect driving safety. The sudden appearance range represents a situation where a vehicle suddenly appears within the range of another vehicle without a gradual exchange of messages, increasing the chances of attacks or interference.

To address these challenges, we propose a trust-based algorithm relying on a weighted average for inspection (TrustWeightCheck), which integrates trust with dynamic weights for checks, such that the weight of a failed check is increased while the weight of a successful check is reduced without neglecting any result. The algorithm's performance was evaluated under two coverage ranges: 420 meters and 600 meters. The results showed that increasing the range slightly affects detection performance, with a minor increase in detection time and a limited decrease in F1-Score metrics. However, the proposed algorithm outperformed others in detection speed, achieving an average detection time of 0.13 seconds along with a high F1-Score rate of 58%. Despite higher entropy in identifying the attacking vehicle due to pseudonym changes that reduce traceability, the algorithm demonstrated a good balance by relying on all checks compared to algorithms based on a single criterion, neighbor trust, or preliminary attack type predictions.

Key Words: Misbehavior detection، VANETs، attack، checks false positives.

***Professor, Faculty of Information and Communication Technology Engineering, Tartous University, Tartous, Syria.**
****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[2]**

١- مقدمة

تعد شبكات العربات اللاسلكية (Vehicular Ad-hoc Networks - VANETs) من المكونات الأساسية لأنظمة النقل الذكية(Intelligent Transport Systems -ITS) ، إذ تلعب دورا محوريا في تعزيز السلامة المرورية، وتحسين التنقل، وتقليل الازدحام في المدن والريف. تعتمد هذه الشبكات على تبادل معلومات لحظي بين العربات (Vehicular to Vehicular-V2V) وبين العربات والبنية التحتية المحيطة مثل وحدات الطريق الجانبية(Vehicular to Infrastructure-V2I) ، عبر رسائل تعرف برسائل السلامة الأساسية (Beacon) تحتوي هذه الرسائل على معلومات مهمة عن حالة العربة وموقعها وسرعتها وتسارعها، ما يساعد في اتخاذ قرارات فورية لتفادي الحوادث والتكيف مع الظروف المرورية[1] .

تعتمد فعالية VANETs بشكل كبير على دقة وموثوقية البيانات المتبادلة. غير أن الطبيعة المفتوحة للشبكة واعتمادها على الاتصال اللاسلكي يعرضها لهجمات سيبرانية تهدد خصوصية وسلامة المستخدمين. من هنا ظهرت أهمية تطوير آليات لكشف السلوكيات المشبوهة أو الخبيثة داخل الشبكة [26],[22].

تتعرض رسائل التبيين لنوعين رئيسيين من الهجمات:

هجمات الخصوصية :يحاول المهاجم تتبع حركة العربات عبر ربط المعرفات الزائفة(Pseudonyms) ، ما يشكل تهديدا مباشرا لخصوصية السائقين. رغم وجود آليات تغيير دوري للأسماء المستعارة، إلا أن تغيير الهوية يجب أن يتم في أوقات وأماكن مناسبة لضمان فاعليته، ولهذا ظهرت استراتيجيات مثل تغيير الهوية في مناطق المزج (Mix-Zones) أو مناطق الصمت(Silent Periods) [24].

هجمات سلامة البيانات : تشمل إرسال بيانات كاذبة من مهاجمين يمتلكون شهادات رقمية وأسماء مستعارة قانونية، مثل هجمات الموقع المزيف، السرعة غير المنطقية، التزاحم المزيف، وهجوم .Sybil تهدف هذه الهجمات إلى تضليل العربات المجاورة مما قد يسبب حوادث خطيرة [25] .

للتصدي لهذه التهديدات، تستخدم منظومات توقيع رقمي تعتمد على بنية المفاتيح العامة (PKI) لضمان مصداقية الرسائل. ولكن، بما أن المهاجم قد يستخدم شهادات مسروقة أو صالحة، فإن التحقق من التوقيع وحده غير كاف. هنا يبرز دور أنظمة كشف سوء السلوك(Misbehavior Detection Schemes -MBDS) ، التي تحلل محتوى الرسائل لرصد أي سلوك غير طبيعي.

اعتمدت معظم أنظمة الكشف عن سوء السلوك على قيام العقدة بعدة فحوصات منها فحوصات المعقولية التي تختبر هل قيم الرسالة الواردة ضمن حدود المعقولة أو لا, حيث يتم تطبيق فحوصات المعقولية على رسالة beacon واحدة على خلاف فحوصات التطابق والتي تستدعي تقييم القيم على رسالتين beacons الحالية والسابقة وذلك لمعرفة هل حدث اختلاف ام لا في القيم, وتعتبر خوارزمية العتبة Threshold Algorithm [22]من أولى الخوارزميات التي اعتمدت على هذه فحوصات وتعتبر الخوارزمية أن فشل إحدى هذه الفحوصات يشير الى أن رسالة سيئة السلوك , لكن في الحقيقة ليس من الضروري أن يكون الفشل احدى الفحوصات مؤشر لوجود سلوك سيء. لذلك اقترحت خوارزمية القيم التجمعية أن يتم تجميع القيم لكل فحصفي سجل متضمن n قيمة لكل فحص و من ثم يحسب متوسط حسابي لهم ,ثم مقارنة النتيجة مع عتبة ثابتة في حال كانت أقل من العتبة , يتم اعتبار الرسالة سيئة السلوك . على الرغم من فعالية هذه الخوارزمية إلا انها ستفشل في بداية المحاكاة والسبب يعود الى أنها ستبقى قيمة القيمة المجمعة

لكل فصأقل من العتبة حتى يمتلئ السجل أو قد تغادر العربة المرسلة مجال تغطية العربة المستقبلة قبل امتلاء السجل بالقيم . استفادت خوارزمية السلوكية من فحوصات المعقولية والتطابق من أجل مراقبة سلوك العربة عن طريق اعطاؤها مهلة زمنية , في حال تجاوزت المهلة ومازال سلوكها سيء , تعتبرها عربة مهاجم , على رغم من أن آلية عمل الخوارزمية تعتبر جيدة كونها لا تحكم على الرسالة إنها قادمة من عربة مهاجمة مباشرة وإنما بعد مرور انتهاء المهلة الزمنية ,لكنها غير مناسبة في شبكات VANET, كون العربة تتحرك وقد تصبح خارج منطقة تغطيتها قبل انتهاء المدة الزمنية . رغم أن الخوارزميات السابقة تملك عيوب ولكنها لا تقارن في عيوب خوارزمية التعاونية التي يعتمد قرارها على حساب ثقة الجيران وثقتها بالرسالة الواردة اليها , وخاصة عند تنفيذ هجومSybil, لذلك تعتبر خوارزميات التي يعتمد قرارها على نفسها أفضل .

على اعتبار أن المتوسط الموزون يعطي أوزاناً لقيم معينة عن غيرها وذلك حسب أهميتها , لذلك اقترحت الدراسة [29] الاستفادة من المتوسط الموزون وتطبيقه على الفحوصات, إلا أنها تستدعي هذه الخوارزمية معرفة مسبقة بنوع الهجوم المقام ليتم زيادة وزن الفحوصات و يتم حساب متوسط الموزون لفحوصات الهجوم المتوقع فقطومن ثم مقارنة القيمة النهائية للمتوسط الموزون بعتبة ثابتة بغضالنظر عن بقية الفحوصات , استفادت الدراسة [28] من المبدأ المعتمد في الدراسة السابقة لكنها أدخلت المتوسط الموزون في معادلة تعزز أو تخفّض قيمة الثقة تدريجياً, لكن أيضاً ارتبطت الثقة بنوع الهجوم المتوقع دون الأخذ بعين الاعتبار بقية الفحوصات. لذلك تم اقتراح خوارزمية تربط بين مفهوم الأوزان الديناميكية للفحوصات ومعادلة الثقة من خلال منح كل فصوزناً متغيراً يتأثر مباشرة بالقيمة التي ينتجها الفصنفسه، دون ربط مسبق بنوع معين من الهجوم. هذا التكيف الديناميكي يسمح بتحسين دقة التصنيف والتعامل بمرونة أكبر مع سيناريوهات الهجوم المتغيرة. لقد حققت الخوارزمية المقترحة قدرة على تصنيف رسائل الهجوم بشكل صحيح بنسبة ٣٥.١٨٪ مقارنة مع خوارزميات العتبة و السلوكية والقيم التجمعية وتعاونية وخوارزمية الثقة القائمة المتوسط الموزون للهجوم , بالإضافة إلى تحقيق نسبة أقل من Negative False والتي تشير إلى عدد الرسائل الهجومية التي لم تكتشف بنسبة ١٤.٤١٪ مقارنة ببقية الخوارزميات , كانت سريعة في الاكتشاف بمتوسط زمني قدره ٠.١٣ثانية مقارنة ببقية الخوارزميات, لكنها عانت من نسبة عالية من الإنذارات الكاذبة بنسبة ٣٥.٧٠٪ والسبب في ذلك الى أن وجود فحص واحد فقط قيمته منخفضة بشكل دائم سيرتفع وزنه وبالتالي زيادة المتوسط الموزون وانخفاض الثقة اتجاه واعتبار أن الرسالة رسالة هجومية حتى لو كانت بقية الفحوصات سليمة .

2-هدف البحث

هدف هذا البحثإلى تحليل أداء الخوارزمية المقترحة ضد هجوم Data Replay Sybil وذلك في حال تم أخذ قيمتين للمجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ ٤٢٠متر و ٦٠٠متر ومقارنة أداؤها مع الخوارزميات السابقة .

3- طرائق البحث و مواده

تم إجراء المحاكاة باستخدام إطارVEINS ، وهو إطار متكامل لمحاكاة الاتصالات بين العربات، يعتمد على نموذج محاكاة ثنائي التفاعل يجمع بين محاكي الشبكات القائم على الأحداثObjective) ++OMNeT (Modular Network Testbed in C++ومحاكي حركة المرور SUMO (Simulation of Urban Mobility).وتم اختيار VEINS نظراً لقدرته على محاكاة الطبقات الكاملة لشبكات الاتصال ٨٠٢.١١ p و(DSRC/WAVE) IEEE 1609.4.

٣-١ أنواع المهاجمين في شبكاتVANET [28]

في شبكات العربات المتنقلة(VANET) ، تختلف أنواع المهاجمين حسب موقعهم في الشبكة وطبيعة نشاطهم، مما يؤثر على قدرتهم في تنفيذ أنواع الهجمات المختلفة. يمكن تصنيف المهاجمين إلى:

- المهاجم الداخلي (Internal Attacker) :عضو مصادق داخل الشبكة، يملك صلاحيات وإمكانيات تمكنه من إرسال وتعديل الرسائل، مما يجعله قادراً على تنفيذ هجمات معقدة تشمل تزوير الهوية والبيانات والتشويش على القناة.
- المهاجم الخارجي External Attacker :كيان خارج النظام، يعمل كمراقب أو متطفل يحاول التشويش أو اعتراض الرسائل، لكنه محدود في قدرته على تعديل البيانات أو انتحال الهوية.
- المهاجم النشط Active Attacker : يشارك بشكل مباشر في الشبكة عن طريق إرسال رسائل مزورة أو تعديل الرسائل الأصلية أو حقن رسائل خبيثة، مما يشكل تهديداً مباشراً.
- المهاجم السلبي Passive Attacker: يقتصر دوره على التنصت على الاتصالات دون تعديل أو التفاعل مع البيانات.
- المهاجم المحلي Local Attacker: ينفذ هجمات في نطاق جغرافي محدود أو ضمن مجموعة عربات محددة.
- المهاجم العام Global Attacker: يمتلك نطاق تغطية واسع، قادر على مراقبة أو مهاجمة الشبكة عبر مناطق متعددة.
- تختلف قدرة كل نوع من المهاجمين على تنفيذ الهجمات حسب هدف الهجوم, ويوضح الجدول (١) أبرز هذه الهجمات:
- الهجمات على قناة الاتصالChannel-based Attacks :يمكن للمهاجمين الداخليين والخارجيين النشطين تنفيذ هجمات إغراق القناة أو التشويش عليها، بينما المهاجم السلبي يقتصر على المراقبة فقط. وتكون هذه الهجمات ممكنة على نطاق محلي أو عام.
- الهجمات على البياناتData-based Attacks :تنفذ عادة بواسطة مهاجمين داخليين ونشطين قادرين على تزوير أو تعديل الرسائل مثل الموقع والسرعة. المهاجم الخارجي لا يملك عادة صلاحية تعديل البيانات، والمهاجم السلبي يراقب فقط.
- الهجمات على الهويةIdentity-based Attacks : غالباً ما يقوم بها مهاجمون داخليون ونشطون يمتلكون صلاحيات انتحال هويات متعددة . المهاجمون الخارجيون يواجهون صعوبة في انتحال الهوية بسبب عدم امتلاكهم هوية معتمدة. المهاجم السلبي غير قادر على تنفيذ هجمات الهوية.

الجدول (١) تصنيف هجمات شبكات VANET وأنواعها

تصنيف الهجوم	اسم الهجوم	وصف الهجوم
Channel-based	DoS Attack	يغمر القناة اللاسلكية برسائل متكررة لتعطيل الاتصال.
	DoS Random	يرسل محتوى عشوائي في فواصل زمنية عشوائية لتشويش الشبكة.
	Disruptive DoS	يعيد المهاجم بث رسائل من جيران عشوائيين بتردد عالٍ

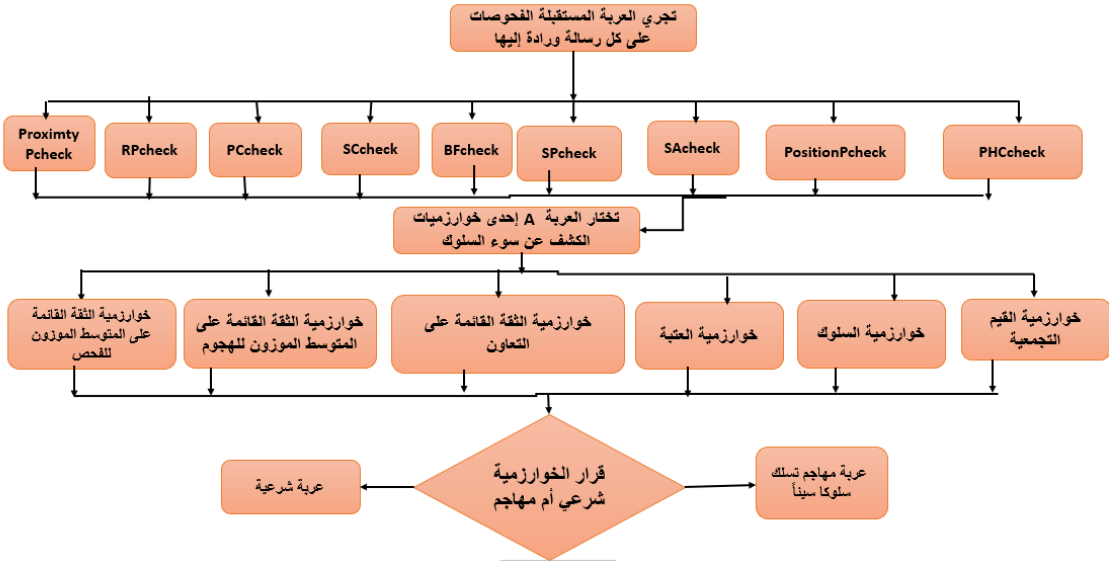
Channel + Identity	DoSRandomSybil	يتم إرسال رسائل تحتوي على قيم عشوائية بتردد مرتفع باستخدام هويات مزيفة مختلفة في كل رسالة.
	DoSDisruptiveSybil	يتم بث رسائل تم استقبالها من جيران مختلفين باستخدام اسم مستعار جديد لكل رسالة
Data-based	Data Replay	يقوم المهاجم بإعادة إرسال الرسائل المستلمة من جار مستهدف معين، بعد توقيعها بشهادته الخاصة
	Disruptive Attack	يعيد المهاجم بث الرسائل التي تم استقبالها من جيران مختلفين
	Eventual Stop Attack	يتصرف المهاجم في البداية كعربة طبيعية، ثم يبدأ ببث موضع ثابت وسرعة صفرية وكأنه توقف فعلياً في مكان ما.
Identity-based	Traffic Congestion Sybil	ينشئ المهاجم ازدحاماً غير واقعي عن طريق توليد عربات وهمية بمعرّفات مزيفة تبث رسائل معقولة بتردد طبيعي من موقع محدد
Identity + Data	DataReplaySybil	يعيد المهاجم بث رسائل مستلمة من جار معين باستخدام عقدة سيبيل

٣-١-١ نموذج المهاجم ضمن العمل

يعد المهاجم الداخلي من أخطر التهديدات الأمنية في شبكات العربات الذكية(VANET) ، نظراً لامتلاكه شهادات رقمية وأسماء مستعارة سليمة تخوله التصرف كعربة شرعية داخل الشبكة. وبفضل هذه الامتيازات، يمكنه إرسال بيانات مزيفة أو التلاعب بعربات أخرى لتنفيذ هجماته، مما يصعب اكتشافه بالاعتماد على تقنيات المصادقة التقليدية فقط. ومن أبرز هذه الهجمات هجوم Data Replay[23][27] Sybil ، الذي يصنف كهجوم مركّب يجمع بين إعادة بث رسائل حقيقية تم التقاطها سابقاً، واستعمال هويات مزيفة متعددة لإيهام النظام بوجود عدة عربات. يهدف هذا الهجوم إلى خلق صورة زائفة لحالة المرور، مما قد يؤدي إلى قرارات خاطئة مثل تغيير المسار أو تقليل السرعة بشكل غير مبرر. ونتيجة لذلك، يعد هذا الهجوم تهديداً مباشراً للسلامة العامة ويقلل من فعالية أنظمة كشف السلوكيات الشاذة في الشبكة.

٣-٢ خوارزميات الكشف عن سوء السلوك

يظهر الشكل (١) المنهجية العامة المستخدمة في الكشف عن سوء السلوك في شبكاتVANET والمعتمدة على فحوصات المعقولية والتطابق , حيث تجري كل عربة مستقبلة الفحوصات على كل رسالة تصلها وتدخل نتائج الفحوصات التي تكون عبارة عن قيم تتراوح بين الصفر والواحد , إلى خوارزميات الكشف المستخدمة , حسب آلية عمل كل خوارزمية يتم اتخاذ القرار بسوء سلوك أو لا . علماً أن نتيجة الفحص كلما اقتربت من الصفر تشير الى فشل الفحص وكلما اقتربت من الواحد, يعتبر الفحص ناجحاً [22]. تقوم العربة المستقبلة بتشغيل إحدى خوارزميات الكشف المبرمجة ضمنها وفق ما يحدده ملف التشغيل omnet.ini.



الشكل (١) ألية اكتشاف سوء السلوك في VANET

٣-٢-١ خوارزمية القيم التجمعية Aggregated Values Algorithm [22]

تقوم العربة بحساب قيمة مجمعة لكل فحص بناء على سجلات الفحوصات السابقة والقيمة الحديثة. تقارن القيمة المجمعة بالعتبة المحددة لاتخاذ قرار حول مصداقية الرسالة وفق المعادلة التالية :

$$IF \quad V_{aggi} = \frac{\sum_i^n V_i + V_{curr_i}}{n+1} < Threshold \quad \rightarrow \quad Misbehavior \quad (1)$$

حيث إن : V_{aggi} : القيمة المجمعة للفحص i الناتجة عن التحديث, V_{curr_i}: القيمة الحالية للفحص i.

تعتمد هذه الخوارزمية بشكل أساسي على أن فشل إحدى الفحوصات المجمعة هو احتمال إلى وجود سوء سلوك.

٣-٢-٢ خوارزمية الكشف السلوكي Behavior Algorithm [22]

تستخدم مهلة الانتظار الزمنية(Timeout Misbehavior Observation–TMO) كأداة رئيسية لمراقبة سلوك كل عربة في الشبكة. يتم حساب عامل الثقة الأدنى (minFactor) الذي يعكس موثوقية رسالة العقدة، ثم يتم تحديث قيمة TMO الخاصة بالعقدة تدريجياً وفق المعادلة (٢) مع كل رسالة يتم استقبالها, حيث تكون قيمتها في البداية هي صفر :

$$\boldsymbol{TMO_i = TMO_i + TMO_{add}} \quad (2) \quad \boldsymbol{where\ TMO_{add} = \alpha e^{\beta(1-minFactor)}}$$

ثم تقارن القيمة TMO_i مع عتبة ثابتة, في حال تجاوز العتبة , يتم اعتبار العربة مشبوهة و يتم تفعيل الإبلاغ عنها. حيث إن α : تمثل معامل ثابت يمثل القيمة الأساسية للإضافة الزمنية, β معامل التضخيم الأسي, وبالتالي الهدف من التحديث التدريجي هو تراكم الشك تجاه العربة.

٣-٢-٣ خوارزمية العتبة Threshold Algorithm [22]

تصف خوارزمية العتبة العربة كمهاجم إذا فشلت أي فحص بغض النظر عن نجاح بقية الفحوصات وكانت نتيجة الفحص C_i أقل من العتبة المحددة θ وفق العلاقة (٣):

$$For\ C_i < Threshold \quad Misbehivor \quad \{where\ C_i \in \{C_1, C_2, \ldots.\}\} \qquad (3)$$

٣-٢-٤ خوارزمية القائمة على الثقة التعاونية Cooperative Algorithm [22]

تدمج الثقة المحسوبة ذاتيا والثقة المستلمة من الجيران لتقدير موثوقية العقدة كما هو واضح بالمعادلتين(٤)(٥). إذا كانت الثقة أقل من الحد المسموح به، تصنف العربة كمشبوهة ويتم الإبلاغ عنها.

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

$$Trust\ level = Trust\ level_{now} + \quad Trust\ level_{neighbors} < \theta \quad Misbehavior \quad (5)$$

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

٣-٢-٥ خوارزمية الثقة القائمة على المتوسط الموزون للهجوم: Trust weighted attack [28]

تطبَّق فحوص متعددة على كل رسالة، وتحسب الثقة باستخدام متوسط موزون ،حيث يعطى كل فحص وزناً مختلفاً حسب نوع الهجوم المكتشف. تم الاستفادة من الدراسة المرجعية[29] في توزيع الوزن وفق هجوم المقام وادخال المتوسط الموزون الناتج إلى معادلة الثقة . يتم حساب مستوى الثقة بالمعادلة (٧)مستخدما معادلة متوسط الموزون للهجوم(٦) :

$$\textbf{Weight Average} = \frac{\sum_{i=1}^{n} \mathbf{w_i} * \mathbf{x_i}}{\sum_{i=1}^{n} \mathbf{w_i}} \qquad (6)$$

حيث إن x_i : قيمة الفحص i ، w_i : وزن الفحص i حسب الهجوم المقام .

$$\textbf{Trust level} = -\frac{\mathbf{e}^{(10(1-\textbf{Weight Average}_{attack})} + \mathbf{1}}{\mathbf{2 * 10^4}} < \theta \quad Misbehavior \quad (7)$$

٣-٢-٦ خوارزمية الثقة القائمة على المتوسط الموزون للفحص المقترحة : Trust weighted Check

الخوارزمية المقدمة هي جزء من نظام كشف سوء السلوك في شبكات العربات الذكية(VANETs) باستخدام آلية غير تعاونية تعتمد على فحوصات متعددة وأوزان ديناميكية لتقييم موثوقية الرسائل المستلمة من العربات الأخرى. تبدأ الخوارزمية بتجميع نتائج الفحوصات (مثل تقارب الموقع، اتساق السرعة، كشف التوقف المفاجئ) لكل رسالة BSM واردة. يتم تمثيل نتيجة كل فحص بالمتغير $C_i \ni [0, 1]$ والتي تعكس درجة مصداقية الرسالة حسب ذلك الفحص, كما تم تخصيص وزن ديناميكي لكل فحص يرمز له بـ $w_i \ni [0, 1]$, يحسب المتوسط الموزون لجميع الفحوصات باستخدام المعادلة(٦). تعدل الأوزان المرتبطة بالفحوصات اعتماداً على فعاليتها في كشف حالات سوء السلوك كما في العلاقة (٨)؛ فإذا أسفر الفحص عن نتائج منخفضة، مما يشير إلى دوره في الكشف، يعزَّز وزنه. أما إذا كانت نتائجه مرتفعة باستمرار، فيخفض وزنه نظراً لضعف مساهمته في عملية الكشف.

$$if \begin{cases} C_i <= \theta_{low} & w_i \rightarrow w_i + \Delta w \\ C_i > \theta_{high} & w_i \rightarrow w_i - \delta w \end{cases} \quad where \quad \theta_{low} = 0.5, \theta_{high} = 0.8, \Delta w = 0.05, \delta w = 0.02 \ (8)$$

حيث إن Δw تمثل قيمة زيادة الوزن , بينما δw قيمة خفض الوزن, و θ_{low} , θ_{high} هما حدود لتقييم الفحص. ثم تحسب معادلة الثقة وفق العلاقة (٩)، وإذا كان مستوى الثقة أقل من عتبة محددة (Threshold)، تعتبر العربة عربة مهاجم . تم اعتماد القيم السابقة وفقاً للتجربة .

$$\textbf{Trust level} = -\frac{\mathbf{e}^{(10(1-\textbf{Weight Average}_{check}))}+\mathbf{1}}{\mathbf{2}*\mathbf{10^4}} < \theta \quad Misbehavior \quad (\mathbf{9})$$

علماً أن الفرق بين خوارزمية الثقة القائمة على متوسط الموزون للفحص بين المعتمدة على متوسط الموزون للهجوم, كلاهما يستخدم المتوسط الموزون وادخال قيمته إلى معادلة الثقة ,لكن الخوارزمية المقترحة تعدل الأوزان ديناميكياً بناء على أداء كل فحص بمرور الوقت وليست بحاجة لمعرفة نوع الهجوم , بينما خوارزمية الثقة القائمة على المتوسط الموزون للهجوم تستخدم أوزاناً ثابتاً محددة مسبقاً حسب نوع الهجوم المتوقع مما يجعلها أقل تكيفاً.

٣-٣ اختبارات المعقولية والتطابق [11]:

تقوم كل عربة عند استقبال رسالة Beacon بإجراء سلسلة من فحوصات المعقولية والتطابق للتحقق مما إذا كانت الرسالة الواردة تعكس سلوكاً سليماً أم سلوكاً سيئاً. في إطار دراسة هجوم Data Replay Sybil، تم التركيز بشكل خاص على فحصي معقولية المجال الأعظمي والظهور المفاجئ ، نظراً لتأثيرهما المباشر على اكتشاف هذا النوع من الهجمات. يوضح الجدول (2) البارامترات الخارجية التي تؤثر على نتائج الفحوصات، والتي بدورها تلعب دوراً حاسماً في دقة اتخاذ القرار من قبل خوارزميات الكشف، اعتماداً على نوع الهجوم المحتمل[29] كما هو موضح في الجدول(3) .

الجدول (٢) البارامترات الثابتة المؤثرة على نتيجة الفحص

الفحص	الاختصار	البارامترات التي تؤثر على الفحص	دلالة البارامتر
فحص معقولية التقارب *Proximity Plausibility Check* يتحقق من قرب العربة من موقع منطقي بالنسبة للمستقبل.	**Proximity Pcheck**	**MAX_PROXIMITY_RANGE_L**	تشير إلى المسافة القصوى في الاتجاه الطولي.
		MAX_PROXIMITY_RANGE_W	تشير إلى المسافة القصوى في الاتجاه العرض
		MAX_PROXIMITY_DISTANCE	تشير إلى المسافة القصوى التي يمكن أن يتفاعل فيها كائنين أو أكثر في النظام
فحص معقولية المجال *Range Plausibility Check* يتحقق من أن موقع العربة يقع ضمن نطاق تغطية الاستقبال المنطقي	**RPcheck**	**MAX_PLAUSIBLE_RANGE**	تشير الى مجال التغطية الأعظمي المعقول
فحص تطابق الموقع *Position Consistancy Check* يتحقق من أن موقع العربة يتغير بشكل منطقي وغير مفاجئ, وذلك من خلال حساب المسافة بين موقعي	**PCcheck**	**MAX_PLAUSIBLE_SPEED**	تشير الى السرعة القصوى المعقولة والمسموح بها على الطريق.

العربة المرسلة السابق والحالي , في حال كانت المسافة أقل من جداء السرعة القصوى المعقولة في الزمن , فموقع العربة منطقي و العربة تتحرك بشكل منطقي.			
فحص تطابق السرعة *Speed Consistancy Check* يتحقق من أن السرعة متطابقة وغير متغيرة بشكل غير منطقي.	**SCcheck**	**MAX_PLAUSIBLE_ACCEL**	التسارع الاعظمي المعقول المسموح به
		MAX_PLAUSIBLE_DECEL	التباطؤ الأعظمي المعقول المسموح به.
فحص معقولية السرعة *Speed Plausibility Check* تحقق من أن السرعة المعلنة لا تتجاوز حدود السرعة الفيزيائية الممكنة.	**SPcheck**	**MAX_PLAUSIBLE_SPEED**	تشير الى السرعة القصوى المعقولة والمسموح بها على الطريق.
فحص الظهور المفاجئ *Sudden Appearance Check* يكشف عن العربات التي تظهر فجأة في النطاق دون اشعار سابق بوجودها داخل مجال التغطية للعربة.	**SAcheck**	**MAX_SA_RANGE**	مجال الظهور المفاجئ الاعظمي.
فحص معقولية الموقع *Position Plausibility Check* يتحقق من أن الموقع المعلن يتوافق مع الواقع ولا يحتوي على قفزات غير منطقية	**PositionPcheck**	**MAX_NON_ROUTE_SPEED**	الحد الأقصى للسرعة التي يمكن اعتبارها معقولة إذا كانت العربة خارج المسار المحدد
		MAX_DISTANCE_FROM_ROUTE	حد أقصى لمسافة يمكن اعتبار العربة عندها قريبة بما يكفي من المسار المتوقع

فحص تردد beacon ***Beacon Frequency Check*** تحقق من أن العربة ترسل رسائل Beacon بتردد مقبول وغير مفرط.	**BFcheck**	**MAX_BEACON_FREQUENCY**	تردد Beacon الأعظمي المسموح به
فحص تطابق اتجاه الموقع ***Position Heading Consistancy Check*** يتحقق من تطابق اتجاه الحركة مع تغير الموقع الفعلي للعربة	**PHCcheck**	**POS_HEADING_TIME**	الزمن المسموح به لتغير اتجاه العربة.
		MAX_HEADING_CHANGE	زاوية تغيير الاتجاه الأعظمي المسموح بها.

يوضح الجدول (٣) الفحوصات التي تكشف الهجوم [23]

الهجوم	**الفحوصات التي تكشف الهجوم**
DoS, DoS Random Attack	فحص تطابق الموقع وتردد رسالةBeacon
DoS Random Sybil Attack	فحص معقولية السرعة و معقولية المجال الأعظمي وفحص الظهور المفاجئ
Disruptive Attack	فحص معقولية الموقع
Dos Disruptive Attack	فحص تطابق الموقع و فحص التقاطع و تردد رسالةbeacon
Data Replay	معقولية الموقع و فحص التقاطع
Data Replay Sybil, Dos Disruptive Sybil Attack	معقولية السرعة و معقولية المجال الأعظمي والظهور المفاجئ و فحص التقاطع.
Eventual Stop	فحص الظهور المفاجئ و فحص معقولية التقارب
Traffic Congestion Sybil	معقولية الموقع و معقولية السرعة و فحص التقاطع

أن هذه البارامترات تأخذ قيم ثابتة في ملفالتشغيل omnet.ini ، لكن لم يتم دراسة فعالية هذه القيم ومدى تأثيرها على دقة الكشف, تمت دراسة تأثير مجال الأعظمي المعقول ومجال الظهور المفاجئ على أداء الخوارزميات في هذه الدراسة بحالة تنفيذ هجومData Replay Sybil.

٣-٤ مقاييس الكشف :[22][29][28][23]

٣-٤-١ التأخير المطلق لكل هجوم (Absolute Latency Per Attack)

هو الزمن المستغرق من لحظة بداية الهجوم (أو لحظة رصده/إرساله) حتى لحظة اكتشافه أو الاستجابة له. تعطى علاقته كما في معادلة (١٠):

$$\text{Absolute Latency Per Attack} = \frac{attackerAverageReportDelay * reportedAttackerNum + deltaTime}{reportAttackerNum + 1} \quad (10)$$

يمثل attackerAverageReportDelay المتوسط الحالي لزمن الإبلاغ عن الهجوم.حيث يدل reportAttackerNum على عدد المهاجمين الذين تم الإبلاغ عنهم حتى الآن، بينما deltaTime هو الزمن الجديد الذي يضاف، وهو الوقت المستغرق للإبلاغ عن هجوم جديد. تعتبر خوارزمية الكشف فعالة عندما يكون الزمن الكلي للاستجابة للهجوم (Absolute Latency Attack) منخفضا، مما يدل على سرعة الكشف، وتتأثر هذه القيمة بنوع الهجوم وكفاءة الخوارزمية.

F1-Scor ٣-٤-٢

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

$$F1 - Score = 2 * \frac{Recall * Precision}{Recall + Precision} (11)$$

٣-٤-٣ الانتروبيا

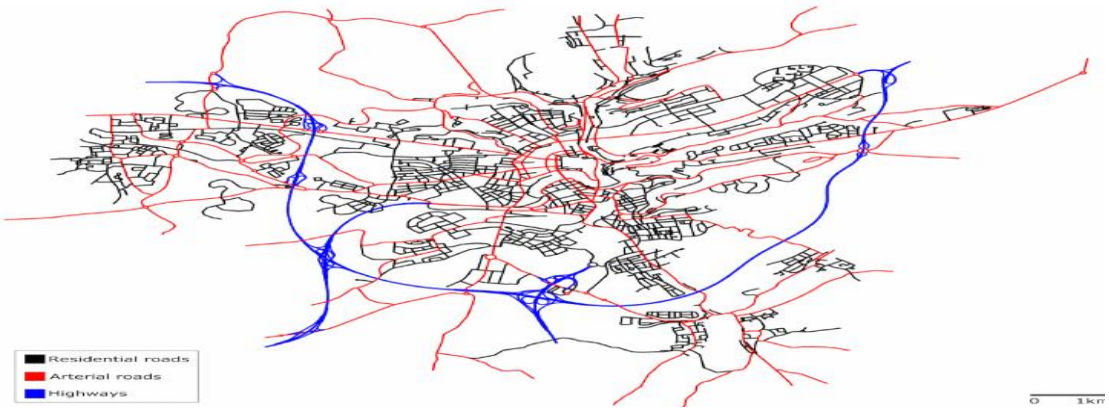
لفهم مقدار الشك (Entropy) لدى الخوارزمية في تصنيف العربات (هل هي شرعية أم مهاجمة)، نستخدم مفهوم الانتروبيا من نظرية المعلومات، والتي تحسب على الشكل التالي:

$$\boldsymbol{H = -P_1 log_2(P_1) - P_2 log_2(P_2)} \quad \boldsymbol{(12)}$$

حيث تمثل $\boldsymbol{P_1}$: نسبة العربات التي تم الإبلاغ عنها على إنها شرعية الى إجمالي العربات, $\boldsymbol{P_2}$: نسبة العربات التي تم الإبلاغ عنها على إنها مهاجم الى إجمالي العربات . تمثل قيمة الإنتروبيا درجة العشوائية أو الارتباك في عملية التصنيف، فكلما كانت القيمة أكبر، دل ذلك على وجود شك عالي في تمييز العربات الشرعية من المهاجمة، مما يشير إلى أداء تصنيف أقل دقة. أما القيم الأقل من الإنتروبيا فتدل على ثبات ودقة أعلى في التصنيف، مما يعكس وضوحا أكبر في تمييز الفئات.

٣-٥ النتائج والمناقشة

من أجل اختبار أداء الخوارزميات السابقة في الزمن الحقيقي , تم اختيار إحدى المدن التي توفر معلومات مرورية مباشرة , إضافة لتحقيق درجة التعقيد والمحاكاة الحقيقة للأداء و بناء عليه تم تحميل مدينة لوكسمبورغ على محاكي Sumo [12], باستخدام بارامترات المحاكاة الموضحة في الجدول (٤) . تم اختيار كثافة الهجوم بحدود ٥٠٪ من مجمل الاتصالات الموجودة في الشبكة خلال مدة المحاكاة ٤ ساعات بحيث تشمل التوقيت بين الساعة ٨ صباحاً وحتى ١٢ ظهراً, حيث تحاكي كثافة مرورية عالية إلى متوسطة تقريبا خلال هذه الفترة.



الشكل (٢) محاكاة لوكمسبورغ [12]

الجدول(٤) بارامترات المحاكاة المستخدمة فيOMNET

Module	Parameter	Value
Veins	Transmission Power	**20mW**
	Bit Rate	**6Mbps**
	Packet Header length	**80bit**
	Beacon Payload length	**100 byte**
	Beacon rate	**1 HZ**
Attacks Parameters	كثافة الهجوم	**50%**
Detection Parameters	**MAX_PLAUSIBLE_RANGE** **MAX-sudden-RANGE**	**600،420 m** **600,420 m**

يجب أن يكون مجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ متساوين القيمة ، وذلك لإنه إذا كان مجال الظهور المفاجئ أكبر من المجال الأعظمي المعقول للتغطية، سترفض الرسائل الشرعية لأنها تبدو وكأنها جاءت من بعيد رغم أنها ضمن مجال الظهور المفاجئ .

تمت محاكاة جميع الخوارزميات التي تم طرحها في الفقرة (٣-٢) ومقارنتها بالخوارزمية المقترحة. تمت المحاكاة بالزمن الحقيقي , لذلك تم أخذ قيم متوسط حسابي لكل من الانتروبيا و F1-Score وزمن اكتشاف الهجوم. يوضح الجدول (٥) نتائج المحاكاة للخوارزميات المدروسة .

الجدول (٥) نتائج المحاكاة للخوارزميات المدروسة .

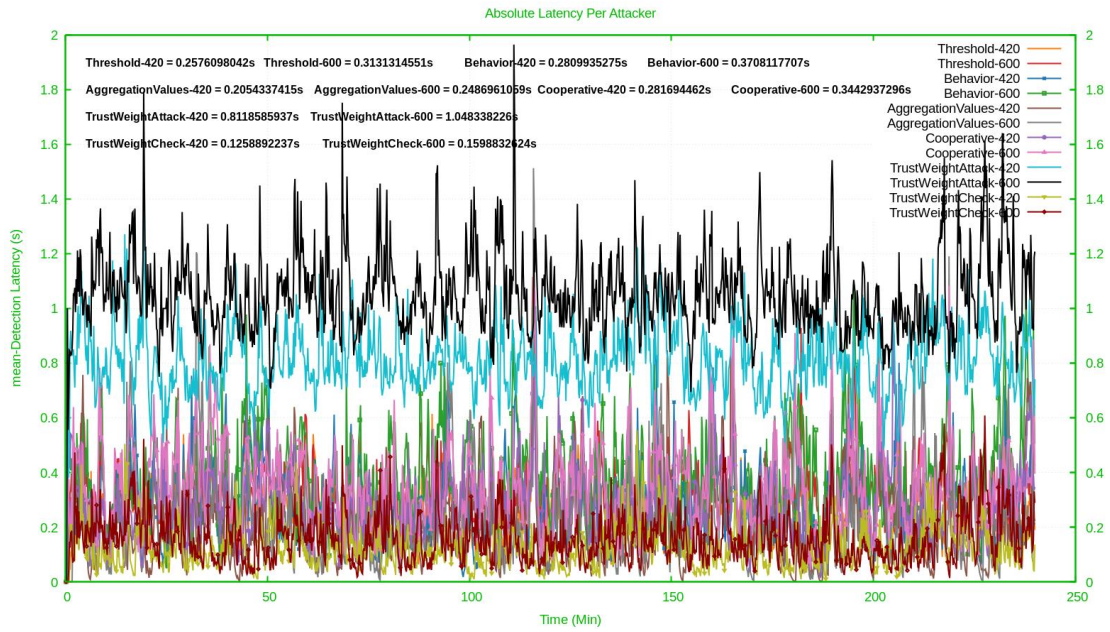
Algorithm	FP%	TN%	TP%	FN%	Average Entropy	Average F1-Score	Average Detection Latency (s)
Threshold_420	0.52	٤٩,٨٨	١٤,٧٢	٣٤,٨٨	٠,٨٩	٠,٤٦	٠,٢٦
Threshold_600	٠,٤٩	٤٩,٩١	١٢,٥٤	٣٧,٠٦	٠,٩٣	٠,٤١	٠,٣١
Behavior_420	١,٩٨	٤٨,٤٢	١٠,١٤	٣٩,٤٧	٠,٨٥	٠,٣٣	٠,٢٨
Behavior_600	١,٦٤	٤٨,٧٨	٧,٨٤	٤١,٧٤	٠,٩١	٠,٢٧	٠,٣٧
AggerationValues_420	٠,٠٩	**٥٠,٣٠**	١٢,١٨	٣٧,٤١	**٠,٥٣**	٠,٤١	٠,٢١
AggerationValues_600	٠,٠٧	٥٠,٣٣	٩,٨٤	٣٩,٧٥	٠,٥٧	٠,٣٤	٠,٢٥
Cooperative_420	٧,٩٣	٤٢,٤٧	٢١,٢٨	٢٨,٣١	٠,٨٦	٠,٥٥	٠,٢٨
Cooperative_600	٧,٤١	٤٣	١٧,٦٧	٣١,٩٢	٠,٩١	٠,٤٨	٠,٣٤
TrustWeightAttack_420	٣٤,١	١٦,٢٤	١٧,٤٧	٣٢,١١	٠,٨٧	٠,٣٤	٠,٨١
TrustWeightAttack_600	٢٩,٦١	٢٠,٧٨	١٣,٣٨	٣٦,٢١	٠,٧٨	٠,٢٩	١

TrustWeightCheck_420 المقترحة	٣٥,٧٠	١٤,٧٠	٣٥,١٨	١٤,٤١	٠,٩٧	٠,٥٨	٠,١٣
TrustWeightCheck_600 المقترحة	٣١,٠٧	١٩,٣٤	٣٠,٨٢	١٨,٧٧	٠,٩٦	٠,٥٥	٠,١٦

يوضح الشكل (٣) زمن اكتشاف الهجوم لكل خوارزمية مدروسة؛ حيث يمثل المحور الأفقي (X) الزمن، بينما يمثل المحور العمودي (Y) زمن اكتشاف الهجوم, كلما اقتربت قيمة زمن الاكتشاف من الصفر، كانت الخوارزمية أسرع في اكتشاف الهجوم. تم رسم هذا المخطط باستخدام بيانات من الزمن الحقيقي، مع احتساب المتوسط الحسابي لقيم كل خوارزمية خلال فترة المحاكاة. تشير النتائج إلى أن زيادة المجال الأقصى المقبول للتغطية أو لمجال الظهور المفاجئ تؤدي إلى زيادة في زمن اكتشاف الهجوم، نتيجة تزايد عدد الرسائل المستلمة عند مسافة ٦٠٠ متر مقارنة بـ ٤٢٠ متر. كما يظهر في الشكل، جميع الخوارزميات تظهر تذبذباً في زمن الاكتشاف، ويعزى ذلك إلى طبيعة شبكة VANET الديناميكية، حيث قد تصف الخوارزمية رسالة معينة على أنها صادرة من عربة شرعية في لحظة معينة، ثم تكتشف بعد فترة أن الرسالة التالية من نفس العربة تحتوي سلوكاً هجومياً، مما يرفع زمن الاكتشاف.

وقد عانت خوارزمية الثقة القائمة على المتوسط الموزون للهجوم TrustWeightAttack ، من تأخير مرتفع للكشف عن الهجوم في حالتي ٤٢٠ متر و٦٠٠ متر، نظراً لاعتمادها على تحديد نوع الهجوم أولاً ثم تعيين الأوزان المناسبة. أما خوارزميتي Behavior وCooperative، فقد أظهرتا زمن اكتشاف متقارب عند مجال ٤٢٠ متر، وذلك بسبب إعطاء خوارزمية Behavior مهلة للعربة لتحديد سلوكها، بينما تعتمد الخوارزمية التعاونية على تقييم ثقة الجوار بالإضافة إلى حساب الثقة الذاتية، مما يزيد من زمن الاكتشاف. بشكل عام، كلما زاد المجال ازداد معه زمن اكتشاف الهجوم.

تعد الخوارزمية المقترحة TrustWeightCheck الأسرع بين جميع الخوارزميات في اكتشاف الهجوم، ويعزى ذلك إلى اعتمادها على آلية ذكية لتعديل الأوزان بشكل ديناميكي وفعال.



الشكل (٣) زمن اكتشاف الهجوم لخوارزميات الكشف عن سوء السلوك بحالة مجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ٢٠٤و٠٠٦متر

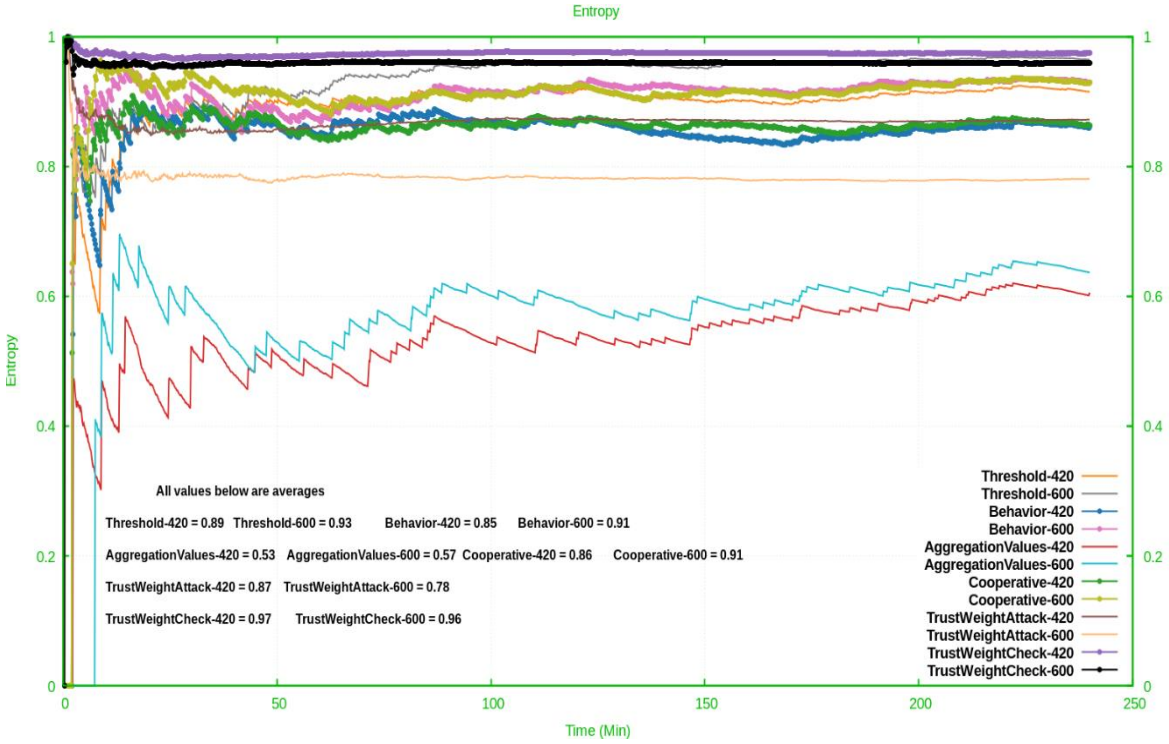
يوضح الشكل (٤) مقدار الشك الناتج عن تصنيف العربة سواء كانت شرعية أو مهاجمة للخوارزميات المدروسة خلال مدة المحاكاة.

في بداية المحاكاة، تعاني جميع الخوارزميات من مستوى مرتفع من الانتروبيا نظراً لقلة البيانات وتضارب المؤشرات، إلا أن هذا الشك ينخفض تدريجياً مع مرور الوقت نتيجة تراكم المعلومات وتحسن عملية التقييم.

مع توسع المجال الأعظمي المعقول للتغطية و مجال الظهور المفاجئ، يزداد تدفق الرسائل في الشبكة، مما يرفع مستوى الشك بالنسبة لمعظم الخوارزميات. ويستثنى من ذلك الخوارزميات المعتمدة على الأوزان، حيث تظهر سلوكاً معاكساً؛ فمع اتساع المجال، تنخفض الانتروبيا نتيجة اعتمادها على الأوزان التي يتم تعيينها إما حسب الهجوم أو حسب قيمة الفصر. لكنها مازالت تبدي الخوارزمية المقترحة أعلى مستويات الانتروبيا مقارنة بباقي الخوارزميات، بسبب لجوء العربة إلى الحصول أولاً على ثقة من خلال اتباع سلوكاً طبيعياً في البداية وبعد مرور فترة زمنية معينة تبدأ تدريجياً ببث سلوك سيئاً عن طريق إعادة ارسال الرسائل التي استقبلتها في الشبكة من عربات شرعية لكن بأسماء مستعارة جديدة .

تظهر خوارزمية الثقة القائمة على المتوسط الموزون للهجوم مستوى أقل من الانتروبيا مقارنة بالخوارزمية المقترحة ، كونها تعطي أوزاناً أعلى للفحوصات التي ساهمت في كشف الهجوم، بدلاً من التعامل مع جميع الفحوصات بنفس الأهمية كما تفعل الخوارزمية المقترحة. أما الخوارزمية التعاونية، فتتأثر بدرجة ثقة الجوار في تحديد هوية العربة. ومع اتساع المجال، تزداد احتمالات تضارب الآراء بين العربات المجاورة، مما يؤدي إلى ارتفاع في مستوى الشك,

تعد خوارزمية القيم التجميعية الأقل شكاً من بين الخوارزميات، نظراً لاعتمادها على سجل ثابت للقيم الخاصة بكل فحص ومقارنتها مع عتبة محددة. هذا النهج الثابت في التحليل يساعد على تقليل التذبذب وبالتالي خفض الانتروبيا.

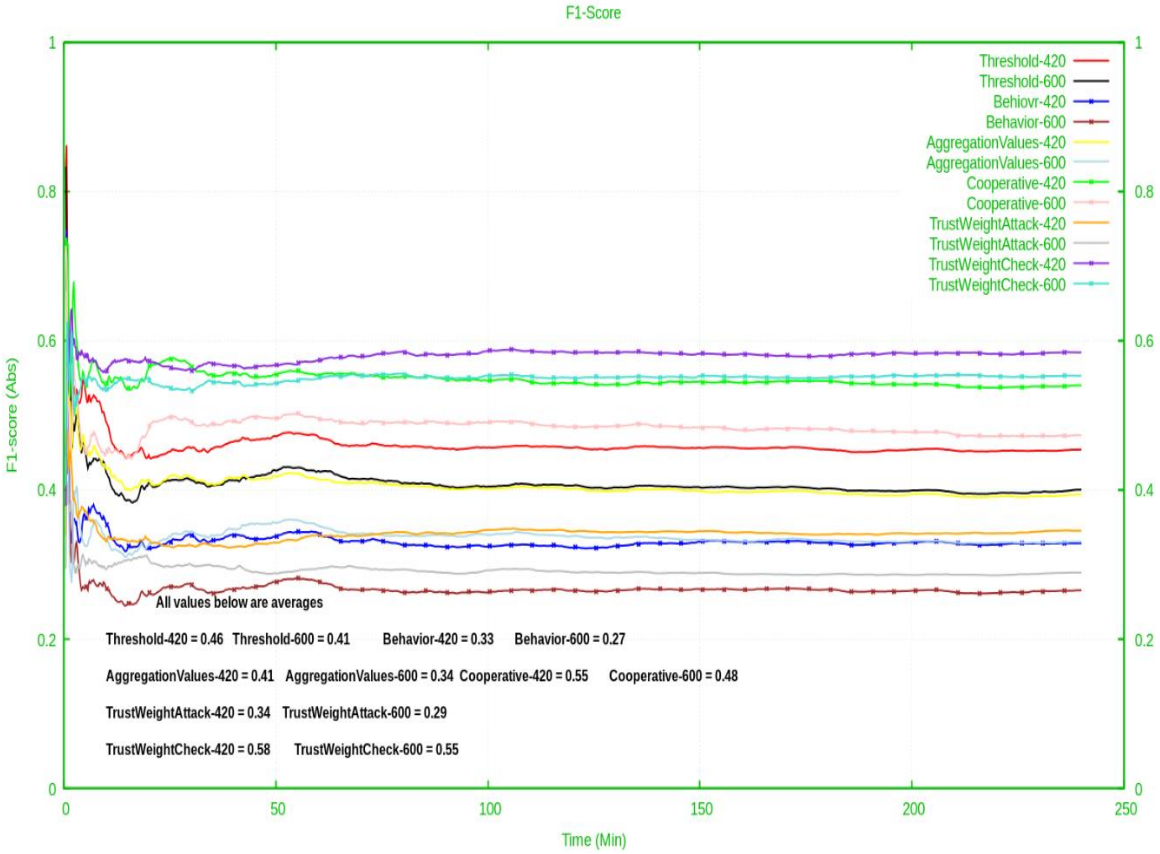


الشكل (٤) الانتروبيا لخوارزميات الكشف عن سوء السلوك بحالة مجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ ٤٢٠و٦٠٠متر

يعرض الشكل (٥) قيم مقياس F1-Score للخوارزميات المدروسة ضمن بيئة المحاكاة أثناء الزمن الحقيقي. تظهر النتائج أن جميع خوارزميات الكشف تبدأ بقيم F1-Score مرتفعة في بداية المحاكاة، ثم تنخفض تدريجياً مع مرور الوقت. يعزى هذا الانخفاض إلى ازدياد تعقيد البيانات وتداخل سلوكيات العربات في بيئة VANET الديناميكية.

كما لوحظ أن F1-Score ينخفض مع زيادة كل من المجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ يعود السبب في ذلك إلى زيادة عدد الرسائل المستلمة من قبل العربة المتلقية، مما يؤدي إلى ارتفاع عدد الرسائل التي لم تصنف بدقة، وبالتالي حدوث اختلال في التوازن بين مقاييسي الدقة (Precision) والاسترجاع(Recall) .

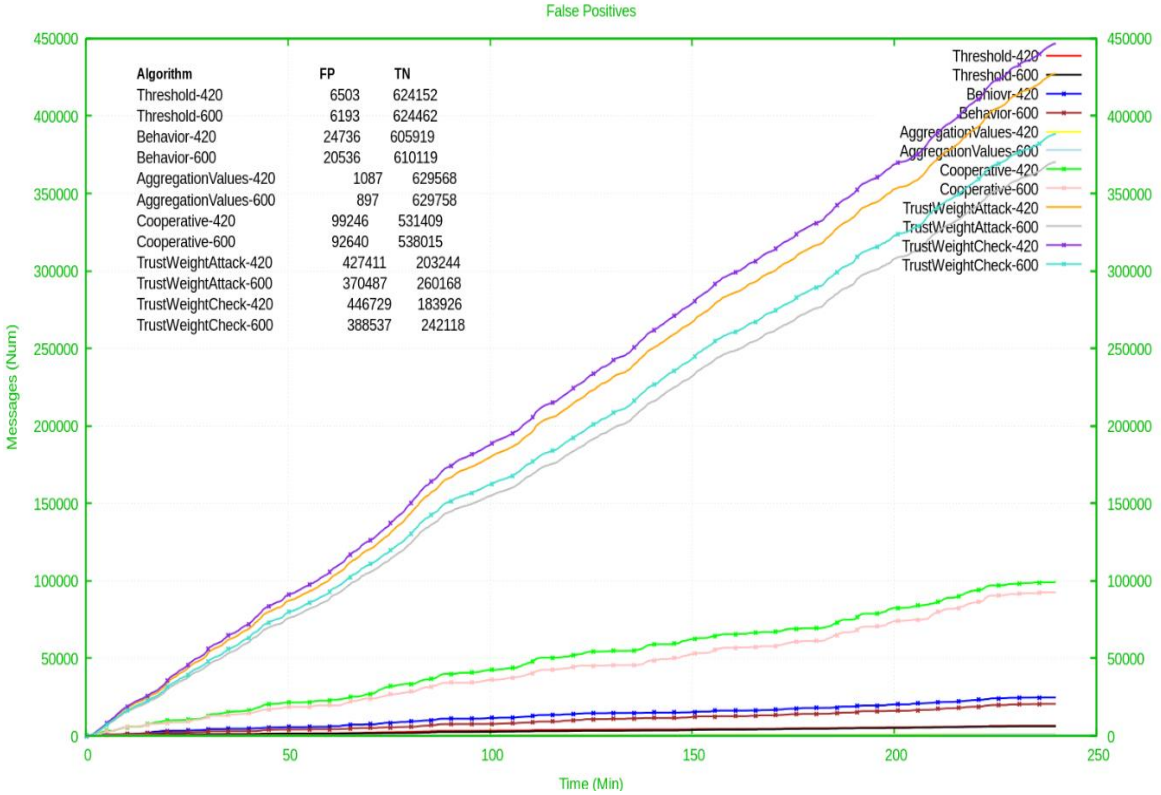
حققت الخوارزمية المقترحة TrustWeightCheck أعلى قيمة لمقياس F1-Score ، مما يدل على استقرار أدائها النسبي مقارنة بالخوارزميات الأخرى. ويعزى هذا التفوق إلى اعتماد الخوارزمية على آلية ذكية في توزيع الأوزان على نتائج الفحوصات، إضافة إلى منح كل فحص نفس الأهمية، دون الاعتماد على مهلة زمنية محددة، أو على نتيجة فحص واحدة، أو على الجوار الذين قد يكون لبعضهم سلوك عدائي أو تصنيف هجومي خاطئ. هذا النهج يقلل من فرص إعطاء تقديرات ثقة خاطئة، مما يساهم في الحفاظ على مستوى مرتفع من F1-Score .



الشكل (٥) مقياسF1-SCOR لخوارزميات الكشف عن سوء السلوك بحالة مجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ٤٢٠و٦٠٠متر

يوضح الشكل (6) تطور عدد الإنذارات الكاذبة (False Positives) المكتشفة خلال الزمن الحقيقي، حيث تبدأ بقيمة صفرية ثم تزداد تدريجياً مع تقدم المحاكاة. عند زيادة كل من مجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ من 420متر إلى ٦٠٠ متر أي بزيادة قدرها نحو 42.86%، لوحظ انخفاض في معدل الإنذارات الكاذبة، حيث تراوحت نسبة الانخفاض من 0.03% في خوارزمية العتبة إلى 4.63% في الخوارزمية المقترحة TrustWeight Check.

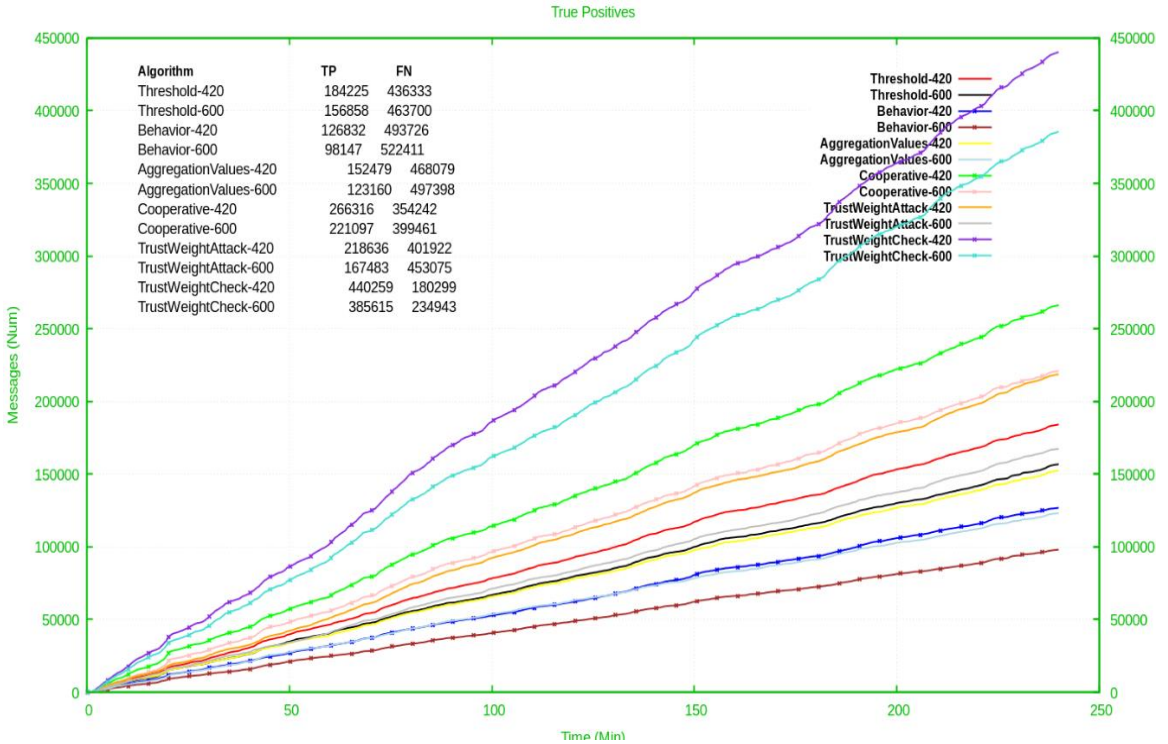
بالمقابل، أدى هذا التوسيع في المجال إلى تحسن في معدل تصنيف الرسائل الصادرة من عربات شرعية بشكل صحيح (True Negative)، إذ زادت النسبة ما بين 0.03% لخوارزمية العتبة وحتى 4.64% للخوارزمية المقترحة. والسبب عائد إلى اعتماد الخوارزمية المقترحة TrustWeightCheckعلى تحديثالأوزان التراكمية لكل عربة مرسلة بناء على الفحوصات المتعددة المستلمة مع مرور الوقت، بحيث يتم تقييم كل رسالة جديدة بناء على مدى توافقها مع القيم السابقة، مما يسمح للنظام ببناء ثقة تدريجية في أن الرسائل واردة من عربات شرعية. على العكس من ذلك، تعتمد خوارزميات أخرى مثل العتبة أو السلوكية على فحصمنفرد أو مهلة زمنية أو تذبذ نوعي للهجوم أو على التعاون فقط، مما يقلل من دقة التصنيف في تلك الحالات.



الشكل (٦) قيم FP للخوارزميات الكشف عن سوء السلوك بحالة مجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ٤٢٠و٦٠٠متر

يوضح الشكل (٧) تطور قيم True Positives (TP) للخوارزميات المدروسة خلال الزمن الحقيقي، حيث تبدأ هذه القيم بالزيادة تدريجياً مع تقدم فترة المحاكاة، وهذا يعكس تحسن الخوارزميات في الكشف عن الهجمات أو السلوكيات المشبوهة بمرور الوقت. عند زيادة مجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ من ٤٢٠ متر إلى ٦٠٠ متر، لوحظ انخفاض في قيم TP بنسب تتراوح بين ٢.١٨٪ في خوارزمية العتبة وحتى ٤.٣٦٪ في الخوارزمية المقترحة TrustWeightCheck, يعود ذلك إلى أن زيادة المجال تسمح باستقبال رسائل أكثر من عربات شرعية، مما يجعل الخوارزميات أكثر تحفظاً في إطلاق الإنذارات، فيقل بذلك عدد TP بالمقابل، زادت قيمFN (عدد الرسائل الهجومية التي لم يتم اكتشافها) بنفس نسب الانخفاض فيTP ، وهذا متوقع لأن انخفاض TP يعني وجود المزيد من الهجمات التي لم يتم كشفها .هذا التوازن يعكس أثر تحديث الأوزان التراكمية في الخوارزمية المقترحة TrustWeightCheck . عانت الخوارزمية المقترحةTrustWeightCheck من زيادة ملحوظة في قيمTP مقارنة ببقية الخوارزميات, السبب عائد إلى اعتمادها على قيمة كل فص, حيث استقرار الفص سيجعلها تخفض وزنه و بالتالي التأثير على قيمة المتوسط الموزون ومنه التأثير على قيمة الثقة المحسوبة ومنه على القرار المتخذ بحق الرسالة ومقارنة مع العتبة التي تتخذ القرار وفق قيمة فص دون أهميته التراكمية لذلك ستزيد قيمFP لديها بشكل أعلى مقارنة ببقية الخوارزميات ,لكن خوارزمية القيم التجميعية AggerationValues رغم اعتمادها على فكرة تراكمية القيم لكل فص واتخاذ القرار وفقاً لفشل إحدى تراكميات الفحوصات ألا إنها كانت أقل خوارزمية تصنف بشكل صحيح و تعاني من عدم قدرتها على تصنيف رسائل الهجومية بنسبة عالية 39.75% مقارنة ببقية

الخوارزميات, هذا الأمر قد يؤثر سلباً على سلامة الشبكة كونها تمرر نسبة عالية من الرسائل الهجومية وتعدّ برها رسائل شرعية .



الشكل (٧) قيم TP للخوارزميات الكشف عن سوء السلوك بحالة مجال الأعظمي المعقول للتغطية ومجال الظهور المفاجئ٤٢٠و٦٠٠متر

٤- الاستنتاجات والتوصيات

تمت محاكاة أداء عدة خوارزميات تشمل: خوارزمية العتبة Threshold، الخوارزمية السلوكية Behavior،خوارزمية القيم التجميعية AggerationValues الخوارزمية التعاونية Cooperative، خوارزمية الثقة القائمة على المتوسط الموزون للهجوم TrustWeightAttack، والخوارزمية المقترحة(خوارزمية الثقة القائمة على متوسط الموزون للفحص)TrustWeightCheck وذلك ضمن حالتي مجال التغطية الأعظمي المعقول ومجال الظهور المفاجئ بقيمتي ٤٢٠ متر و٦٠٠ متر.

أظهرت النتائج أن زيادة المجال من ٤٢٠م إلى ٦٠٠م أدت إلى ارتفاع طفيففي تأخير اكتشاف الهجمات (Detection Latency) في جميع الخوارزميات، باستثناء خوارزمية الثقة القائمة على المتوسط الموزون للهجوم، حيث بلغ مقدار الزيادة في التأخير حوالي 0.19 ثانية، ويعزى ذلك إلى اعتماد هذه الخوارزمية على توقع نوع الهجوم أولاً ثم توزيع الأوزان وفقاً له.

كذلك، لوحظ انخفاض بسيط في قيمة F1–Score مع ازدياد المجال، إلا أن الانخفاض كان أقل ما يمكن في الخوارزمية المقترحةTrustWeightCheck ، مما يشير إلى حفاظها على توازن جيد بين معدلات الكشف والدقة.

أما من حيث الانتروبيا(Entropy) ، فقد أظهرت الخوارزميات التقليدية ازدياداً في قيم الشك مع زيادة المجال، بينما أظهرت الخوارزميات المعتمدة على الأوزان، انخفاضاً في الانتروبيا بمقدار 0.01 للخوارزمية المقترحة مقابل 0.09 في خوارزمية الثقة القائمة على المتوسط الموزون للهجوم، مما يشير إلى تحسن في استقرار الثقة

بالقرارات.كذلك تأثرت مؤشرات التصنيف بزيادة المجال , حيث أدت الزيادة إلى انخفاض عدد الرسائل الهجومية المكتشفة بشكل صحيح نتيجة زيادة عدد العربات داخل المجال وازدياد حجم الرسائل .بالإضافة الى انخفاض طفيف في قيم الانذارات الكاذبةFP , زيادة في عدد الرسائل الشرعية المصنفة بشكل صحيحTN وزيادة عدد رسائل الهجومية التي لم تكتشف. والسبب عائد إلى ازدياد حجم التبادل داخل المجال الموسع، مما يعزز استلام رسائل صحيحة لكنه يقلل من وضوح مؤشرات الهجوم.

تعتمد الخوارزمية القائمة على المتوسط الموزون للفص على حساب متوسط موزون ديناميكي، حيث يتم تعيين وزن أكبر للفحوص التي تقترب قيمها من الصفر، مما يزيد تأثيرها ويؤدي إلى انخفاض الثقة في الرسالة. أما الفحوص المستقرة والتي تقترب من القيمة ١، فيتم تقليل وزنها دون تجاهلها كلياً، بخلاف خوارزمية الثقة القائمة على المتوسط الموزون للهجوم تعطي الوزن فقط لفحوص محددة حسب نوع الهجوم المتوقع.

وقد حققت الخوارزمية المقترحة:

عدد رسائل المصنفة بشكل صحيح بقيمة35.18% من مجمل الرسائل الهجومية و بالمقابل تقليل عدد رسائل الهجومية التي لم تكتشفها FN بقيمة 14.41% و بينما كانت عدد الإنذارات الكاذبة بحدود٣٥.٧٠٪ , بينما بلغت عدد رسائل شرعية الصحيحةTNبحدود ١٤.٧٠٪ , أي أن الخوارزمية المقترحة متوازنة لذلك أعطت قيمةf1–Score عالي مقارنة مع بقية الخوارزميات رغم ذلك إلا إنها عانت من شك في تصنيف العربات والسبب عائد الى أن العربة تغير اسمها المستعار للحفاظ على شرط الخصوصية وذلك في المجال الاعظمي المعقول للتغطية ومجال الظهور المفاجئ ٤٢٠متر .

يوصى باعتماد خوارزمية الثقة القائمة على المتوسط الموزون للفص TrustWeightCheckكأساس لنظام كشف الهجمات .بالإضافة إلى :

- إجراء اختبارات إضافية في بيئات محاكاة واقعية لتقييم الأداء بشكل أدق.
- ادخال المرشحات التي تعمل على ازالة القيم الشاذة او اكتشافها إلى خوارزميات الكشف.
- توليد Datasets تكون ناتجة عن دراسة مجمل بارامترات الكشف وإدخالها إلى خوارزميات التعلم الآلي وذلك بهدف تسريع الكشف واتخاذ قرارات دقيقة .

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]Kamel, J., Jemaa, I. B., Kaiser, A., & Urien, P. (2018, December). Misbehavior reporting protocol for c-its. In 2018 IEEE Vehicular Networking Conference (VNC) (pp. 1-4). IEEE

[4] 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.

[5] Pavithra, T., Nagabhushana, B. S., & Das, S. (2022, August). Study of the Impact of Sybil Attack in VANETs Using F2MD. In International Conference on Intelligent Cyber Physical Systems and Internet of Things (pp. 533-543). Cham: Springer International Publishing.

[6] 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.

[7] 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).

[8] 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.

[9] 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.

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

[11] 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.

[12] Z. Elrewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,”Veh. Commun., vol. 23, pp. 1–28, Jun. 2020.

[13] R. Hussain, J. Lee, and S. Zeadally, “Trust in VANET: A survey of current solutions and future research opportunities,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 5, pp. 2553–2571, May 2021.

[14] Kamel, J., Haidar, F., Jemaa, I. B., Kaiser, A., Lonc, B., & Urien, P. (2019, October). A misbehavior authority system for sybil attack detection in c-its. In 2019 IEEE 10th Annual Ubiquitous Computing, \Electronics & Mobile Communication Conference (UEMCON) (pp. 1117-1123). IEEE

[15] Ali Akbar Pouyan and Mahdiyeh Alimohammadi. Sybil Attack Detection in Vehicular Networks. In Computer Science and Information Technology 2.4, pages 197 – 202, 2014. doi: 10.13189/csit.2014.020403.

[16] Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin Shen. Footprint: Detecting sybil attacks in urban vehicular networks. IEEE Transactions on Parallel and Distributed Systems, 23(6):1103–1114, June 2012. ISSN 2161-9883. doi: 10.1109/TPDS.2011.263.

[17] Rens W van der Heijden et al. “Survey on misbehavior

detection in cooperative intelligent transportation systems”. In: arXiv preprint arXiv:1610.06810 (2016).

[18] Norbert Bißmeyer et al. “Central misbehavior evaluation for vanets based on mobility data

plausibility". In: 9th ACM Workshop on vehicular inter-networking, systems, and applications. 2012.

[19] Chen Chen, Xin Wang, Weili Han, and Binyu Zang. A robust detection of the sybil attack in urban vanets. In 2009 29th IEEE International Conference on Distributed Computing Systems Workshops, pages 270–276,June 2009. doi: 10.1109/ICDCSW.2009.48

[20] Soyoung Park, Baber Aslam, Damla Turgut, and Cliff C. Zou. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In MILCOM 2009 - 2009 IEEE Military Communications Conference,pages 1–7, Oct 2009. doi: 10.1109/MILCOM.2009.5379844.

[21] Yong Hao, Jin Tang, and Yu Cheng. Cooperative sybil attack detection for position based applications in privacy preserved vanets. In 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, pages 1–5, Dec 2011. doi: 10.1109/GLOCOM.2011.6134242.

[22] Clavijo-Herrera, M., Banda-Almeida, J., & Iza, C. (2021, November). Performance evaluation in misbehaviour detection techniques for DoS attacks in VANETs. In Proceedings of the 18th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks (pp. 73-80).

[23] Sultana, R., Grover, J., Tripathi, M., & Sharma, P. (2024). LA-DETECTS: Local and Adaptive Data-Centric Misbehavior Detection Framework for Vehicular Technology Security. IEEE Open Journal of Vehicular Technology.

[24] Shaleesh, I. S., Almohammedi, A. A., Mohammad, N. I., Ahmad, A. A., & Shepelev, V. (2021). Cooperation and radio silence strategy in Mix Zone to Protect Location Privacy of Vehicle in VANET. Tikrit Journal of Engineering Sciences, 28(1), 31-39.

[25] Ayaida, M., Messai, N., Wilhelm, G., & Najeh, S. (2019, June). A novel Sybil attack detection mechanism for C-ITS. In 2019 15th international wireless communications & mobile computing conference (IWCMC) (pp. 913-918). IEEE.

[26] Sangwan, A., Sangwan, A., & Singh, R. P. (2023). A classification of misbehavior detection schemes for VANETs: a survey. Wireless Personal Communications, 129(1), 285-322.

[27] A. Sharma and A. Jaekel, "Machine learning based misbehaviour detection in VANET using consecutive BSM approach," IEEE Open J. Veh. Technol., vol. 3, pp. 1–14, 2021.

[28] Shaleesh, I., Mohammed, N., & Mohammed, G. (2025). A trust algorithm based on weighted average for determining vehicle behavior in VANET. Tartous University Journal for Research and Scientific Studies,9(4).

[29] Sultana, R., Grover, J., & Tripathi, M. (2022, November). A data-centric and dynamic-range based misbehavior detection approach for vanet. In TENCON 2022-2022 IEEE Region 10 Conference (TENCON) (pp. 1-6). IEEE.