

إدارة الثقة في شبكات المركبات باستخدام سلاسل الكتل المستضافة في

السحابة: دراسة أثر الذاكرة المؤقتة في المركبات

د. علي الحاتم*

الملخص

تتلعب VANET دوراً مهماً في دعم نظم النقل الذكي وتعزيز السلامة المرورية من خلال التطبيقات التي تعتمد على تبادل الرسائل بين المركبات والبنية التحتية. نحتاج إلى آليات موثوقة لإدارة الثقة في شبكات VANET للتحقق من المركبات وكشف السلوك الخبيث كونها تؤثر على كل من سلامة المركبات واتخاذ القرار بشكل يهدد حياة مستخدمي مركبات VANET. نقدم من خلال هذا البحث إطاراً متكاملاً لإدارة الثقة في شبكات VANET المعتمدة على سلاسل الكتل السحابية بحيث يتم مراقبة سلوك المركبات وتجميع الأدلة من خلال وحدات (RSUs) Road Side Units، في حين تستخدم سلسلة الكتل لتخزين الأدلة وقرارات الثقة. من خلال هذا الإطار يتم الفصل بين التحقق من الهوية والذي يتم من خلال سلطة الشهادات (CA) Certificate Authority، وبين إدارة الثقة والتي تتم من خلال سلسلة الكتل، وتُمثل حالة المركبة بإحدى الحالات التالية: موثوقة أو مشبوهة أو خبيثة. أظهرت نتائج التقييم تحسن نسبة التسليم (PDR) packet delivery ratio في سيناريو السرعات المتغيرة بينما أثرت على قرار الثقة، كما بينت النتائج أن وجود الذاكرة المؤقتة يسمح بالتوسع في الشبكة ويقلل الاعتماد على وحدات RSU والسحابة، لكنها لا تحسن معدل المنع الفعلي في بيئات متغيرة السرعة وذات كثافة مرورية عالية الأمر الذي يتطلب سياسات متقدمة في تحديث حالات الثقة المخزنة في ذاكرة V2V. الكلمات المفتاحية: شبكات VANET، إدارة الثقة، سلاسل الكتل، الذاكرة المؤقتة V2V.

* عضو هيئة تدريسية في جامعة حمص-كلية الهندسة المعلوماتية - قسم هندسة الشبكات والنظم الحاسوبية

Trust Management in VANETs Using Cloud-Hosted Blockchain: A Study of Cache Impact in Vehicles

Dr. Ali Alhatem*

Abstract

VANETs play an important role in supporting intelligent transportation systems and enhancing traffic safety through applications that rely on message exchange between vehicles and infrastructure. We need reliable mechanisms for trust management in VANETs to verify vehicles and detect malicious behaviour, as it affects both vehicle safety and decision making in a way that threatens the live of VANET vehicle users. In this research we present an integrated framework for trust management in VANETs based on cloud blockchains, where vehicle behaviour is monitored and evidence is collected by Roadside Units (RSUs), while the blockchain is used to store evidence and trust decisions. Through this framework, identity verification which is performed through the Certificate Authority (CA) is separated from trust management, which is performed through blockchain, and which represents the vehicle state as trusted, suspicious, or malicious.

The results showed an improvement in the packet delivery ratio (PDR) in the variable-speed scenario, while it affected the trust decision. The results also showed that the presence of the cache allows scalability in the network and reduces dependence on RSUs and the cloud, but it doesn't improve the

effective prevention rate in variable-speed environments with high traffic density, which requires advanced policies for updating trust states stored in the V2V cache.

Keywords: VANETs, Trust Management, Blockchains, V2V cache.

* Lecturer – Homs University– IT Faculty– Department Of Computer Networks & Systems Engineering

مشكلة البحث:

تتسم VANETs بأنها ذات طبيعة ديناميكية وتتضمن تبادل رسائل حساسة تتعلق بالسلامة المرورية واتخاذ القرار، الأمر الذي يتطلب تجنب السلوك الخبيث للمركبات. تجدر الإشارة إلى عدم كفاية هوية المركبة لضمان الموثوقية فمن الممكن أن يكون للمركبة شهادة صحيحة ولكن ترسل بيانات مزيفة أو تعيد إرسال رسائل قديمة.

تعتمد الكثير من حلول إدارة الثقة في VANETs على التحقق من الهوية أو الخلط بين إلغاء الهوية وإلغاء الثقة أو تتطلب الرجوع إلى جهة مركزية الأمر الذي يزيد من التأخير. توفر سلاسل الكتل سجلاً لا يمكن التلاعب فيه ولكنه في نفس الوقت يضيف عبئاً إضافياً إذا تم الرجوع إليه في كل مرة لمعرفة حالة الثقة. أضف إلى ذلك تؤثر ديناميكية VANETs من جهة حركة المركبات على نسبة تسليم الرزم واستقرار قرارات الثقة.

أهداف وأهمية البحث:

نهدف من خلال هذا البحث إلى كشف السوك الخبيث للمركبات في VANETs بطريقة مستقلة عن هوية المركبة، كما نهدف إلى تقليل الاعتماد على RSUs والسحابة باستخدام آلية تخزين مؤقتة V2V. تكمن أهمية البحث في إيجاد إطار متكامل لإدارة الثقة في VANETs قادر على الفصل بين هوية المركبة وتقييم الثقة بناءً على الأدلة التي يتم تجميعها من قبل RSUs وتخزينها في سلسلة كتل مركزية (في السحابة). كما تمكن أهمية البحث في دراسة نماذج الحركة المتنوعة بوجود الذاكرة المؤقتة وبدون وجودها بما يبرز محاسن ومساوئ تحقيق الذاكرة المؤقتة V2V في الإطار المقترح.

أدوات البحث:

تم اختبار البنية المقترحة من خلال تحقيق شبكة VANET باستخدام محاكي SUMO من أجل كثافات متنوعة من العقد (20,40,60,80,100) بحيث تعكس عدد مركبات قليل ومتوسط وكبير. تم تحقيق طبقات البنية عبر برنامج بايثون يعمل على محاكاة سلسلة الكتل في السحابة ومنح الشهادات الرقمية من قبل CA وتحقيق أربع أنواع من الهجمات.

مقدمة:

تلعب شبكات المركبات VANETs دوراً مهماً في أنظمة النقل الذكية حيث تتيح تبادل الرسائل بين مختلف مكونات هذه الشبكات وأبرزها V2V و Vehicle 2 Infrastructure (V2I) حيث تتيح هذه الوسائل تحقيق العديد من التطبيقات مثل تجنب الازدحام و التحذير من الحوادث و توجيه المركبات والاتصال بالانترنت. نظراً لحساسية بعض التطبيقات التي تدعمها VANETs فإن أي تأخير في

الرسائل أو الرسائل المزيفة أو التلاعب بالهوية أو إعادة استخدام رسائل سابقة قد يؤدي إلى كوارث تؤثر على سلامة مستخدمي هذه المركبات.

تعمل آليات المصادقة على جانب مهم من أمن VANETS من خلال التحقق من هوية المركبات باستخدام الشهادات الممنوحة من قبل CA ولكنها لا تكفي لوحدها بسبب إمكانية أن تقوم مركبة ذات هوية صحيحة بسلوك خبيث كأن ترسل معلومات غير صحيحة مثل الموقع أو السرعة أو تتلاعب بالمعلومات لذلك تتجه الأبحاث نحو دراسة إدارة الثقة بوصفها مكملة لآلية المصادقة ودعم أمان VANETS. تشير العديد من الدراسات إلى أن إدارة الثقة أصبحت جزءاً أساسياً في التصدي للهجمات حيث أن الحلول الحديثة تدمج الثقة و سلاسل الكتل والذكاء الصناعي والخصوصية والتوسع [1].

تتنوع استراتيجيات حساب الثقة والتي يمكن أن تتم باستخدام النماذج الإحصائية [2] أو نظرية الألعاب أو بالاعتماد على الذكاء الصناعي بهدف تقييم موثوقية المركبة أو الرسائل بناءً على السلوك أو التاريخ أو الأدلة المتاحة [7]. قمنا في بحثنا بحساب الثقة بدل الاعتماد على الهوية فقط من خلال تجميع الأدلة بهدف اتخاذ القرار بعد نافذة معينة يتم من خلالها تراكم الأدلة مما يجعل القرار المتخذ أكثر حذراً وتكيفاً.

تتوفر عدة حلول تتناول موضوع التوسع في بيئات تعتمد على سلاسل الكتل تشمل تجزئة سلاسل الكتل وسلاسل الكتل الجانبية وتقنيات الإجماع المحسنة وتخفيض تكلفة الوصول إلى سلسلة الكتل [1][5]. إن عملية الرجوع المستمر إلى سلسلة الكتل أو إدارة السلسلة من قبل RSUs قد يؤدي إلى تأخير وحمل مرتفع [5][6]. من خلال بحثنا حافظنا على مكان سلسلة الكتل وهي السحابة، وتم استخدام آليات لتقليل الرجوع المستمر إلى السحابة وتشمل Trust Token و BloomFilter و RSU Cache و V2V Cache.

هنالك توجهات حديثة للتكامل مع VANETS وتشمل الحوسبة الطرفية والتوأمة الرقمية والتعلم الاتحادي بهدف تقليل العبء وتحسين زمن الاستجابة ودعم التنبؤ تحسين القدرة على التكيف [1]. بشكل مشابه

تقريباً للحوسبة الطرفية قمنا باستخدام RSU كمراقب ومجمع للأدلة [6] واستخدمنا السحابة في تخزين الأدلة وقرارات الثقة.

أكدت الدراسات على أن أنظمة الثقة في VANETs يجب أن تكون آمنة مع المحافظة على الخصوصية بسبب إمكانية اكتشاف كل من هوية المركبة وموقعها واتجاهها [1][8]. قمنا في البحث بتحقيق هذه الاعتبارات الأمنية من خلال تخزين الأدلة وقرارات الثقة في سلسلة الكتل لمنع التلاعب بها، كما تم الفصل بين التحقق من الهوية بجعل CA مسؤولاً عنها وإدارة الثقة في طبقة أخرى.

الدراسة المرجعية:

تعتبر إدارة الثقة في VANETs و Internet of Vehicles (IOVs) من المواضيع الرئيسية لحماية المركبات وضمان موثوقيتها وتبادل الرسائل بشكل آمن. لا تكفي طرق المصادقة التقليدية في اكتشاف سلوك المركبات كون المركبة التي تمتلك هوية صحيحة قد يكون لها سلوك مضلل. أظهرت الدراسات المرجعية أن تقنيات إدارة الثقة في VANETs تعمل على تقييم موثوقية المركبات والرسائل اعتماداً على السلوك وسمعة المركبة والأدلة المجمعة من قبل المركبات أو وحدات RSUs مع إبراز التحديات مثل السرعات العالية وتغيير الطوبولوجيا وقابلية التوسع [1] [2]، حيث تؤكد هذه الدراسات على الحاجة إلى آليات لإدارة الثقة بشكل يمكن معه التعامل مع الرسائل المزيفة والمركبات الخبيثة دون الاعتماد على هوية المركبة فقط.

اتجهت العديد من الأبحاث إلى الاعتماد على سلاسل الكتل في إدارة الثقة بسبب قدرتها على مقاومة التلاعب بالبيانات وإمكانية التتبع وتوفير سجل مشترك من قرارات الثقة. تتركز الأعمال البحثية حول أربعة محاور وهي: طرق حساب الثقة والتكامل مع تقنيات الاتصال الحديثة 5G/6G وقابلية التوسع وآليات الإجماع بالإضافة إلى آليات تتعلق بالأمان والخصوصية [1].

ركزت العديد من الأعمال على بناء آلية للثقة قائمة على سلاسل الكتل لتقييم كل من المركبات والرسائل، حيث اقترح الباحثون في [2] نموذجاً للإدارة الثقة في VANET بالاعتماد على تحليل السلوك وسلسلة الكتل وذلك باستخدام نموذج ماركوف المخفي الذي يعمل على تقييم الثقة ومن ثم حفظ معلومات الثقة في سلسلة الكتل لمنع التعديل. أظهر البحث أهمية الفصل بين هوية المركبة من جهة وسلوكها من جهة أخرى وهنا تم التركيز على حساب الثقة دون التطرق لتأثير التخزين المؤقت في المركبات على كل من قابلية التوسع وتقليل العبء على سلسلة الكتل.

صمم الباحثون في [3] نظام TrCoin يتعامل مع البيانات المزيفة والتغذية الراجعة غير الصادقة عبر خوارزمية تقيس قيمة الأمانة لكل مركبة وتستبعد التغذية الخبيثة قبل احتساب قيمة الثقة النهائية وتخزينها في سلسلة الكتل. كما اقترح [4] نموذج TrustedBlockMCDM الذي يستخدم سلسلة الكتل في اتخاذ قرار يعتمد على معايير متعددة لتحسين الكشف عن الرسائل المزيفة والمركبات الخبيثة في VANETs. تعمل هذه الأبحاث ضمن تحسين دقة الكشف وحساب الثقة دون التركيز على أثر V2V Cache كطبقة تخفف الحمل عن البنية السحابية وسلسلة الكتل.

تناولت بعض الأبحاث مشكلة قابلية التوسع في نظام إدارة الثقة المعتمد على سلاسل الكتل حيث قدم الباحثون في [5] نظام إدارة ثقة في VANETs يدعم قابلية التوسع والموثوقية وعدم التلاعب بالبيانات. أكد البحث على أن نقل كل عمليات الثقة إلى سلسلة الكتل تؤدي إلى عبء مرتفع، وبالتالي تم التركيز على البنية العامة لسلسلة الكتل وقابلية التوسع في حين نركز في بحثنا على V2V Cache مع تحليل المفاضلة بين تحسين معدل تسليم الرزم وتقليل العبء على سلسلة الكتل من جهة، ومعدل المنع الفعلي من جهة أخرى.

اقترحت عدة أبحاث حلولاً أكثر تعقيداً مثل [6] حيث تم اقتراح نموذج ثنائي الطبقة لإدارة الثقة في IOV، طبقة تتضمن سلسلة الكتل للمركبات وأخرى لوحدة RSU. في هذا البحث تم تخفيف العبء وتحسين التوسع من خلال التمييز بين الرسائل المهمة وغير المهمة، وبين القرارات التي تحتاج إلى تسجيل دائم أو التعامل معها محلياً. في بحثنا لا نقترح سلسلة كتل مزدوجة وإنما سلسلة واحدة في

السحابة وندعمها بطبقة V2V و Trust Tokens لتقليل العبء على السحابة. قدم الباحثون في [7] بنية مقترنة بالتعلم العميق تعالج هجمات إعادة الإرسال والانتحال الشخصية والتعديل. يفرض وجود سلسلتي كتل تحديات في تزامن القرار تعالجها بنيتنا المقترحة بوجود سلسلة كتل واحدة مع كاش محلية.

فيما يتعلق بالخصوصية والمصادقة قدم البحث [8] نموذجاً يجمع بين إدارة الثقة بالاعتماد على سلسلة الكتل ومخطط يحافظ على الخصوصية المشروطة حيث يُسمح بإرسال الرسائل برسائل بصورة مجهولة مع مزامنة الرسائل ومصادقتها عبر السلسلة وبذلك لا يتم ربط هوية المركبة بقرارات الثقة مباشرة. في بحثنا قمنا بفصل طبقة الهوية المسؤولة عنها سلطة الشهادات CA عن طبقة الثقة والتي تعمل على تصنيف المركبة حسب سلوكها وتخزين الأدلة وقرارات الثقة عوضاً عن هوية المركبة.

عملت العديد من الأبحاث على توظيف التخزين المؤقت في شبكات المركبات بهدف تخفيف الضغط عن البنية التحتية، إلا أن غالبيتها كان يهدف إلى تخزين المحتوى وليس إدارة الثقة كما في [9]. قدم الباحثون في [10] آلية للتخزين المؤقت بهدف الأمان وتحسين المصادقة وذلك بوجود مخدّم بين المركبات ووحدات RSUs الأمر الذي خفض التكلفة بنسب تتراوح بين 67% و 88%. يعد مرشح Bloom هيكلية بيانية فعالة في الفحص السريع بتكلفة منخفضة وهو ما يجعل استخدامه في VANETs خياراً فعالاً. تم استخدامها من قبل [11] لضغط قوائم الشهادات الملغاة Certificate Revocation List (CRL) بدلاً من نقلها بشكل كامل مما خفض حجم الرسائل. قدم الباحثون في [12] إطار مصادقة خفيف الوزن يجمع بين Tesla ومرشح Bloom لتوليد CRL واستخدم الباحثون في [13] مرشح Bloom للتحقق من حالة الشهادات محلياً في المركبات بدون وجود بنية مركزية. استخدم الباحثون في [14] مرشح Cuckoo بدلاً من مرشح Bloom إذ يدعم الحذف الفعلي للشهادات منتهية الصلاحية ويتجاوز ويتفادى مشكلة الإيجابية الكاذبة التي يعاني منها مرشح Bloom وتناول الباحثون في [15] كيفية توزيع CRL بكفاءة في بنية VANET الهرمية مؤكدين على أن حجم هذه القائمة ينمو خطياً مع عدد الشهادات الملغاة الأمر الذي يستدعي ضغطها.

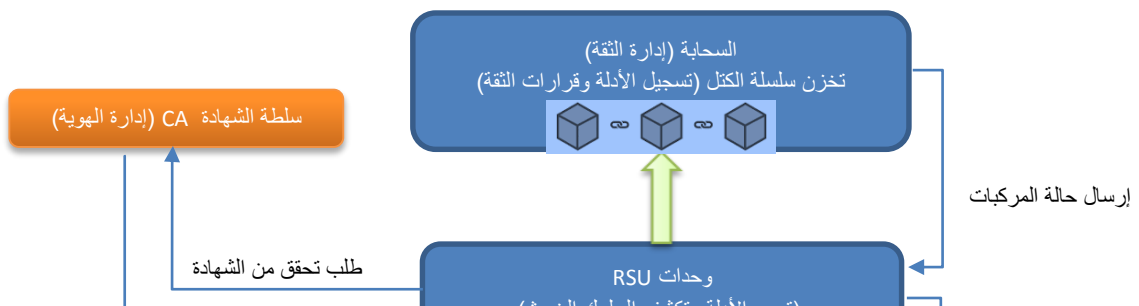
نستخدم مرشح Bloom في بحثنا ليس بهدف ضغط CRL فحسب، بل لتمثيل حالة الثقة الكاملة للمركبات المجاورة. أثبتت نتائج المحاكاة التي قمنا بها نسبة إصابة للكاش بلغت بالمتوسط لجميع التجارب 98.8% مما يؤكد أهمية هذا الاستخدام في تخفيف الحمل بنسبة تتراوح بين 49% إلى 74% حسب كثافة المركبات في الشبكة.

يمكن تلخيص مساهمتنا في هذا البحث من خلال تقديم إطار متكامل لإدارة الثقة في VANETs بالاعتماد على سلسلة كتل سحابية لتسجيل قرارات الثقة مع استخدام V2V Cache لتسريع اتخاذ القرار دون الرجوع الى السحابة. تعمل المنهجية المقترحة على فصل طبقة الثقة عن التحقق من الهوية وتعالج عدة أنواع من الهجمات مثل تزوير بيانات الحركة وإعادة الإرسال والتلاعب بالشهادات و هجوم الإغراق Flooding.

لن نتطرق إلى بنية VANETs أو الحديث عن سلاسل الكتل لوجود العديد من الأبحاث التي تتحدث عنهما، وسيتم التركيز على البنية المقترحة ونتائج التقييم.

المنهجية المقترحة:

سنقوم بالتعبير عن المنهجية المقترحة كما في الشكل (1) الذي يمثل ارتباط طبقات البنية التحتية مع بعضها.



RSU Cache

الشكل (1) الإطار المقترح لإدارة الثقة في VANETs باستخدام سلاسل الكتل

يشتمل الإطار المقترح على طبقات شبكة VANET المعتمدة على السحابة وهي: طبقة المركبات وطبقة وحدة الطريق وطبقة السحابة. تحتوي كل مركبة على ذاكرة V2V Cache تحتوي معلومات عن حالة الثقة للمركبات الأخرى. تحصل المركبة على معلومات الثقة من وحدات RSU التي تقوم بدورها بمراقبة سلوك المركبات وإرسال الأدلة إلى طبقة السحابة التي تقوم بتخزين الأدلة في سلسلة الكتل وحساب حالة الثقة لكل مركبة. سنأتي إلى شرح وظائف كل طبقة على حدى.

1- طبقة المركبات:

تمثل هذه الطبقة مركبات الشبكة والتي تتبادل الرسائل فيما بينها وهذه الرسائل قد تكون طبيعية أو خبيثة مثل رسائل الإغراق. تعتمد المركبات على ذاكرة الكاش V2V Cache للاحتفاظ بحالات الثقة للمركبات المجاورة مما يسمح باتخاذ قرارات أولية محلياً دون الرجوع للسحابة.

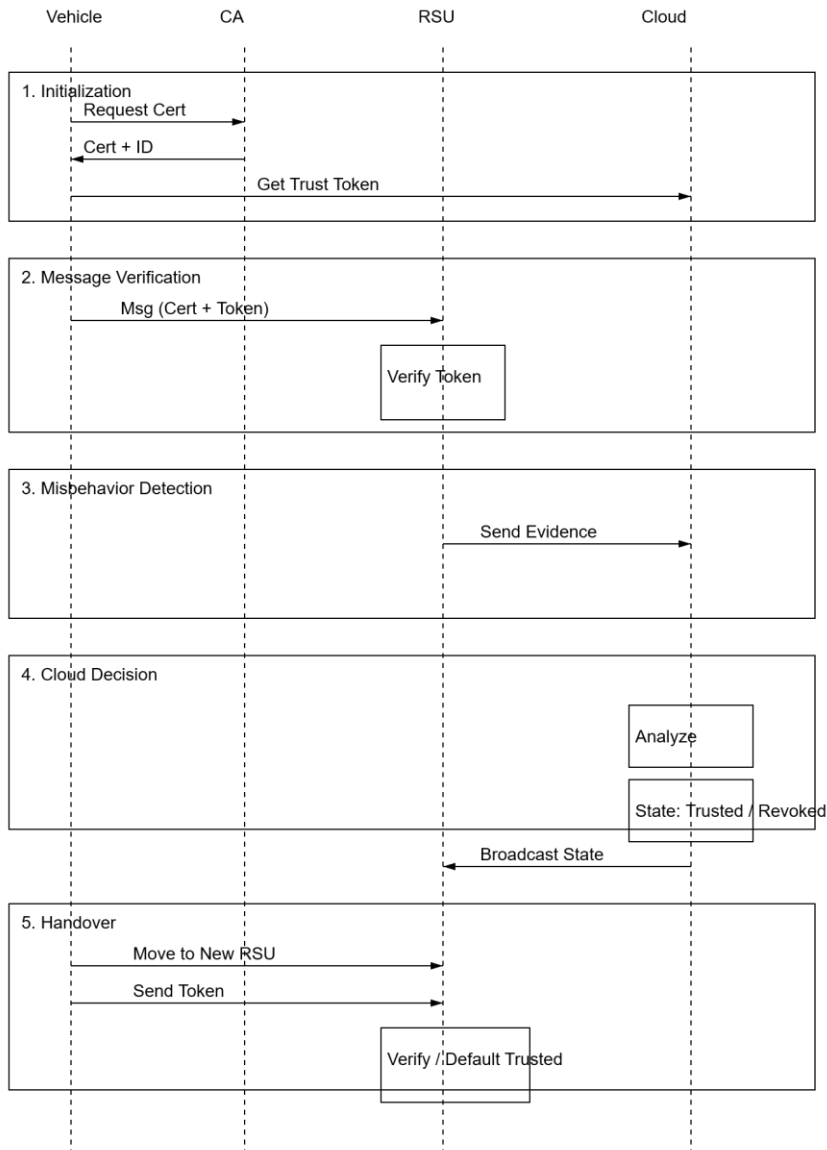
2- طبقة وحدات RSU:

تعمل كوسيط بين طبقة المركبات والسحابة ومهمتها تتمثل في التحقق من هوية المركبات عبر التواصل مع سلطة الشهادات وجمع الأدلة المتعلقة بسلوك المركبة واتخاذ قرارات ثقة أولية محلياً. عند اكتشاف سلوك غير طبيعي تقوم وحدة RSU بإرسال الأدلة إلى السحابة لتسجيلها ضمن سلسلة الكتل، وتقوم أيضاً بتحديث معلومات الثقة للمركبات المجاورة. يتوفر في وحدة RSU ذاكرة تخزين محلية كما يظهر في المخطط، وذلك كون RSU هي التي تستقبل الرسائل ولديها قدرة على تحليل سلوك المركبة واتخاذ قرار سريع. بفرض لم نحقق هذه الذاكرة المؤقتة في RSU سيحدث ضغط كبير في الشبكة يتسبب بتأخير عالٍ وPDR أقل. إن وجود RSU Cache يجعل فرق التأخير في حال وجود V2V Cache ويدونها، قليلاً وهو ما أظهرته التجارب.

3- طبقة السحابة:

تمثل هذه الطبقة مركز إدارة الثقة في الإطار المقترح حيث تحتوي على سلسلة الكتل التي تسجل الأدلة وقرارات الثقة بهدف عدم التلاعب بها. تقوم هذه الطبقة بتحليل الأدلة الواردة من RSU ومقارنتها مع عتبات لتحديد حالة الثقة للمركبة.

إدارة الثقة في شبكات المركبات باستخدام سلاسل الكتل المستضافة في السحابة: دراسة أثر الذاكرة المؤقتة في المركبات



الشكل (2) مخطط تسلسلي يوضح ارتباط مكونات الإطار المقترح

يلخص المخطط التسلسلي في الشكل (2) المنهجية المتبعة في الإطار المقترح لإدارة الثقة في VANETs. في البداية تطلب المركبة شهادة يتم الحصول عليها من CA التي تقوم بدورها بتزويد المركبة بشهادة رقمية موقعة وهوية مخفية. تتواصل المركبة مع السحابة وتحصل على Trust Token في البداية تكون قيمته Trusted أي المركبة موثوقة، وهي الحالة الافتراضية التي تبدأ بها المركبة.

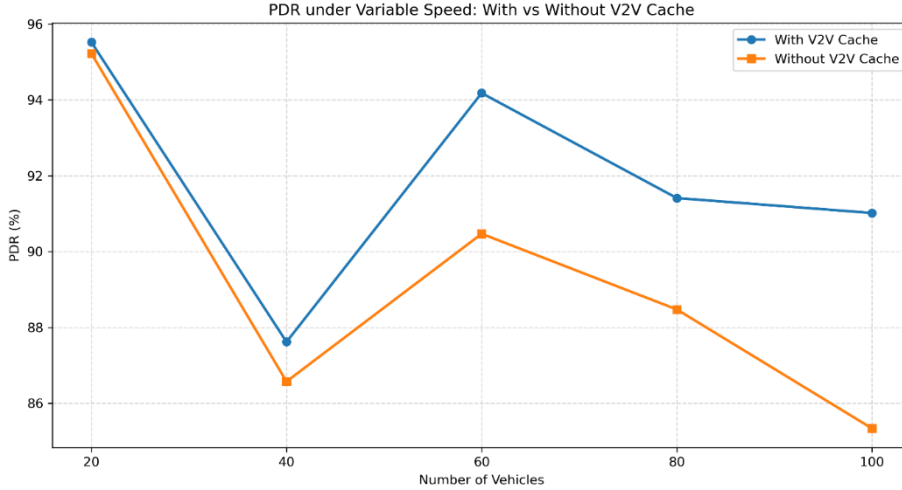
من أجل كل رسالة ترسلها المركبة، تستقبل RSU الرسالة مع الشهادة والرمز. تقوم RSU بالتحقق من الرمز وفي حال كان موثقاً يتم قبل الرسالة الأمر الذي نتجنب من خلاله سؤال السحابة من أجل كل رسالة. بالإضافة إلى عملية التحقق هذه تعمل RSU على مراقبة السلوك. في حال الاشتباه يتم إرسال دليل إلى السحابة، وبالتالي يمكن اعتبار RSU بمثابة المراقب ولكن لا يتخذ أي قرار يتعلق بحالة الثقة للمركبة. من خلال هذا البحث تم التعامل مع عدة أنواع من السلوك الخبيث الذي يمكن للمركبة أن تقوم به وهي: إرسال بيانات غير منطقية مثل السرعة والاتجاه وهجمات إعادة الإرسال وهجوم الإغراق. تجمع السحابة الأدلة من RSUs ويتم تحليلها ضمن نافذة زمنية ومقارنتها مع عتبات محددة وعليه تكون حالة المركبة إما موثوقة (Trusted) أو مشتبهاً بها (Suspected) أو إلغاء الثقة (Revoked).

بعد اتخاذ القرار يتم توزيع الحالة على جميع RSUs ويتم إصدار Token للمركبة. في حال انتقال مركبة من نطاق RSU1 إلى نطاق RSU2 تقوم بإرسال شهادتها والToken إلى وحدة RSU2. تقوم RSU2 بالتحقق من Token في حال كانت صالحة يتم قبول المركبة وفي حال عدم وجود Token يتم اعتبارها موثوقة مؤقتاً وهي ما يعتبر فراغ زمني صغير في الثقة يتطلب معالجته في أبحاث لاحقة.

تحقق المنهجية المقترحة اتصالات من نوع V2V وهنا يمكن اتخاذ قرارات محلية باستخدام V2V Cache. تم تصميم V2V Cache في هذه المنهجية بهدف تحقيق السرعة وتخفيف الحمل بحيث تتضمن المركبات المرفوضة وبالتالي عند استلام مركبة رسالة من مركبة أخرى إذا كانت المركبة المرسله في V2V Cache سيتم رفض الرسالة وإلا يتم قبولها. تجدر الإشارة إلى نقطتين أساسيتين: الأولى إن قبول الرسالة لا يعني أن المركبة المرسله موثوقة بشكل كامل، بسبب ديناميكية الشبكة وتأخر محتمل في تحديث V2V Cache والثانية إن V2V Cache يعتمد على مرشح Bloom filter الذي

قد يُنتج إيجابية كاذبة حيث تصنف بعض المركبات الموثوقة على أنها مرفوضة وذلك بسبب طبيعة عمل هذا المرشح ولكنه يعتبر مقبولاً لعدم وجود سلبية كاذبة بالإضافة إلى الفعالية العالية لهذا المرشح وانخفاض زمن المعالجة.

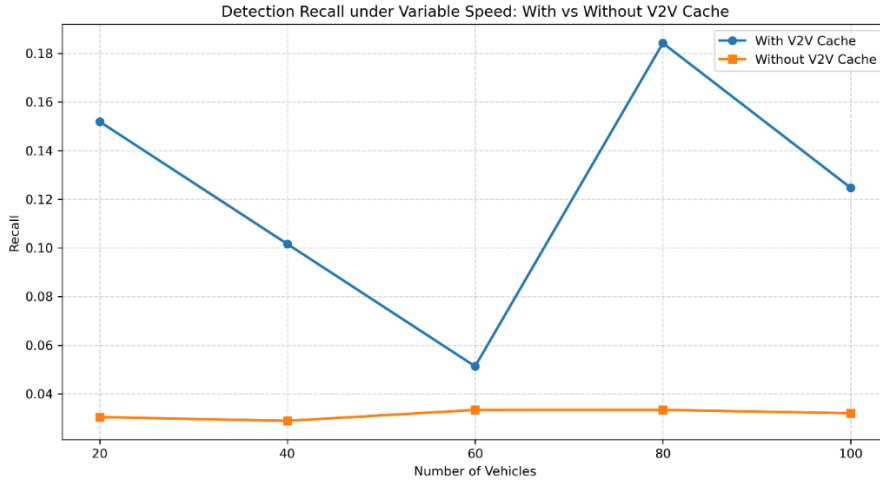
لضمان تخزين الأدلة بشكل غير قابل للتعديل أو التلاعب بالإضافة إلى تحديث حالات الثقة وتسجيل قرارات الحظر. تشكل سلسلة الكتل مرجعاً لحالة كل مركبة، ويتم الرجوع له في الحالات التي تتطلب تأكيد الموثوقية لمركبة ما في حال عدم توفرها في الكاش المحلي.



الشكل (3) معدل تسليم الرزم

يوضح الشكل (3) أثر V2V cache على نسبة تسليم الرزم المقبولة PDR في البيانات التي تكون فيها سرعة المركبات متغيرة وبالتالي أي رسالة لا ترسل أو تستقبل ستؤدي إلى انخفاض هذا المعدل ويشير PDR هنا إلى عدد الرسائل المقبولة بعد تطبيق طبقة الثقة. من أجل سيناريو عدد المركبات القليل 20 مركبة كان PDR مرتفعاً وهي نتيجة منطقية بسبب انخفاض الحمل والحجب على مستوى طبقة الثقة الأمر الذي يجعل عدد الرسائل المرسله يساوي تقريباً عدد الرسائل المستلمة. نلاحظ بوجود الكاش ومن أجل عدد المركبات المتوسطة الكثافة إلى العالية تفوق النموذج الذي يحقق V2V cache كونها تقلل الاعتماد على الـ RSU و السحابة بما يزيد من نسبة تسليم الرزم المقبولة. الانخفاض الواضح عند عدد مركبات 40 كونه مرتبط بقرارات طبقة الثقة وهذا ما تم التحقق منه من جدول النتائج حيث تبين أن عدد الرسائل المفقودة يكافئ عدد الرسائل المحجوبة بسبب الثقة. ولكن تجدر الإشارة إلى أن تحسن قيمة PDR في حالة استخدام V2V cache لا يعني تحسناً في المنع الفعلي إذ أظهرت النتائج أن V2V cache يحتاج إلى سياسات أكثر تكيفاً لتحديث معلومات الثقة. إن انخفاض معدل

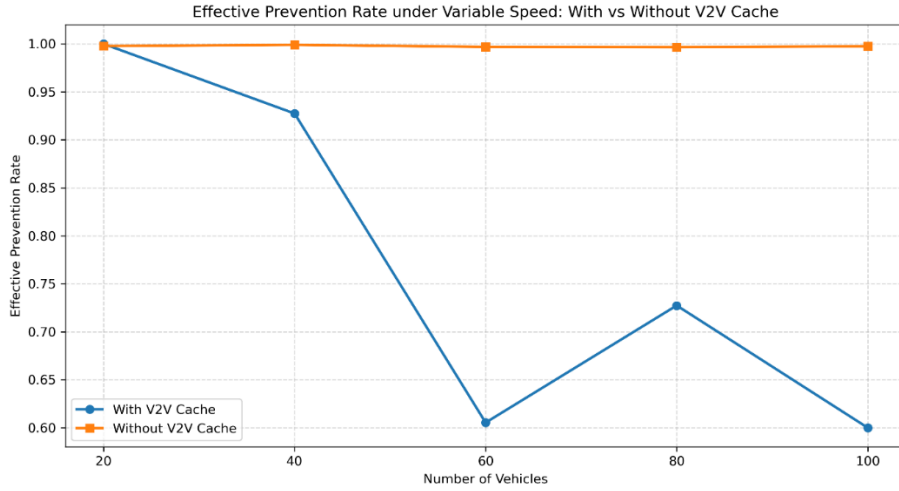
PDR مع زيادة عدد المركبات هو أمر مفهوم كون هذه الزيادة تعني زيادة عدد الرسائل واحتمال الازدحام وتداخل الاتصالات وزيادة عدد الرسائل التي يمكن أن ترفض في طبقة الثقة.



الشكل (4) أثر V2V Cache على مقياس Recall لاكتشاف الهجمات السلوكية

يُظهر الشكل (4) أثر V2V cache على مقياس Recall حيث أظهرت النتائج تحسن ملحوظ من أجل جميع الكثافات من العقد مقارنة مع الحالة التي لا يتوفر فيها V2V cache الأمر الذي يعزز أن تبادل معلومات الثقة مع المركبات يعزز قدرة النظام على كشف السلوك الخبيث. نلاحظ التباين الحاصل في قيم Recall حيث سجلت أعلى قيمة عند 80 مركبة وأقل قيمة عند 60 مركبة ويعزى هذا التباين إلى طبيعة توزيع الهجمات وعدد الاكتشافات المسجلة وآلية المنع عبر الكاش. تجدر الإشارة إلى مقياس Recall يستخدم الاكتشافات الصحيحة للهجمات السلوكية بالنسبة لإجمالي الهجمات السوكية الفعيلة، وبالتالي في السيناريو بدون V2V Cache ستمر الرسائل عبر RSU والسحابة ويتم منع رسائل دون تسجيلها اكتشاف جديد الأمر الذي يفسر القيم المنخفضة لمقياس Recall بدون V2V Cache. نلاحظ انخفاض القيمة المطلقة للـ Recall في الحالتين، حيث بلغت 0.184 عند 80 مركبة كأفضل حال، ويعزى ذلك -كما أشارت إليه العديد من الأبحاث- إلى صعوبة اكتشاف سلوك المركبات في

بيئة VANET الديناميكية. إلى أن المهم في هذا البحث إظهار التحسن الملموس بوجود V2V Cache من عدمه.



الشكل (5) أثر V2V Cache على معدل المنع العام EPR

يوضح الشكل (5) معدل المنع الفعلي وقد أثبتت النتائج أن هذا المعدل بدون V2V cache يكون قريب من الواحد بمعنى منع معظم محاولات السلوك الخبيث في الشبكة. يفسر ذلك كون قرار المنع يتم في السحابة بالاعتماد على حالات ثقة محدثة وبالتالي سيكون قرار المنع أكثر استقراراً. أما في السيناريو الذي يتضمن V2V Cache نلاحظ أن معدل المنع كان عالياً بوجود عدد قليل من المركبات وبدأ بالانخفاض مع زيادة عدد المركبات بسبب التراجع في موثوقية المنع لوجود معلومات غير محدثة في V2V cache الأمر الذي يستدعي البحث عن سياسات لتحديث معلومات الثقة في الكاش.

يجب أن نميز بين المقياسين السابقين لتفسير النتائج، في حين أن مقياس Recall يقيس اكتشاف الهجمات السلوكية كاكشافات صحيحة أما معدل المنع الفعلي يقيس منع المحاولات الخبيثة من التأثير سواءً عن طريق الحظر أو رفض مركبة محظورة أو منع محاولة بعد أن أصبحت مركبة محظورة. لذلك يمكن القول بوجود V2V cache لدينا قيم Recall أعلى لأن نشر حالات الثقة في المركبات

يزيد من الكشف السلوكي، في حين أن معدل المنع الفعلي أقل لأن بعض القرارات قد تعتمد على حالات غير محدثة في الكاش. بالمقابل وبدون وجود V2V Cache تكون قيم Recall منخفضة لأن عدد الاكتشافات السلوكية أقل ويكون معدل المنع أعلى لأن السحابة تمنع المحاولات الخبيثة بصرامة انطلاقاً من حالات ثقة محدثة.

إن معدل المنع الفعال (EPR) Effective Prevention Rate في الشكل (5) يحسب نسبة الهجمات الممنوعة إلى مجموع الهجمات الواصلة إلى RSU وبالتالي يتجاهل الهجمات التي تم منعها في V2V Cache قبل وصولها إلى RSU. سنعمل على تعريف مقياس تقييم يجمع بين المنع على المستوى المحلي والمنع على مستوى سلسلة الكتل بهدف تقييم قدرة النظام الكلية على صد الهجمات، حيث لاحظنا في الأبحاث التي تم دراستها عدم وجود مثل هذا المقياس، كونها تركز على أحدهما.

سندعو المقياس بـ System Prevention Rate (SPR) ويعطى بالعلاقة التالية:

$$SPR = (V2Vp + BCp) / Total_Malicious_Attempts \quad (1)$$

حيث أن V2Vp يمثل الكشف على مستوى V2V cache و BCp يمثل الكشف على مستوى سلسلة الكتل و Total_Malicious_Attempts عدد الهجمات الكلي. تكون قيمة SPR ضمن المجال [0-1]. يقدم الجدول التالي مقارنة بين مقياس EPR و SPR من أجل كثافات مختلفة من المركبات بهدف تبيان مساهمة V2V Cache وسلسلة الكتل في قيمة SPR الإجمالية.

الجدول (1) مقارنة مقياسي EPR و SPR من أجل كثافات متنوعة من المركبات

العدد	EPR بدون V2V	EPR مع V2V	مع SPR V2V	V2V %	BC %	كسب SPR
20	0.997	1.0	1.0	77.1%	22.9%	+0.0
40	0.999	0.927	0.978	70.8%	27.1%	+5.1
60	0.996	0.605	0.823	55.3%	27.1%	+21.8
80	0.996	0.727	0.957	84.3%	11.5%	+23.0
100	0.997	0.600	0.914	78.6%	12.8%	+31.5

يظهر من الجدول (1) أنَّ SPR يصبح صورة EPR الذي يُخفِّق في تمثيل القدرة الفعلية للنظام عند تفعيل V2V Cache مما يوحي بأداء ضعيف لا يعكس الواقع. على سبيل المثال بوجود V2V، يبلغ EPR قيمة 0.6 عند عدد مركبات يساوي 100، في حين قيمة SPR بلغت 0.914 مما يكشف أن 31.5% كانت مخفية عن مقياس EPR كونها تعلقت بمنع محلي قبل الوصول إلى البنية التحتية للشبكة. تُظهر نتائج SPR مساهمة V2V Cache في المنع الكلي والذي يتصاعد مع زيادة عدد المركبات حيث بلغ 77.1% عند 20 مركبة ووصل لـ 84.3% عند 80 مركبة. يعزى الانخفاض عند 60 مركبة إلى حساسية الطوبولوجيا العشوائية عند الكثافات المتوسطة وهو ما يحتاج إلى آلية مخصصة لتحديث الكاش.

يمكننا القول أن مقياس SPR أثبت قدرة النظام على صد هجمات بين 82% إلى 100% في حين أظهر مقياس EPR قدرة النظام على صد هجمات بنسبة 62% إلى 100%، وبالتالي يمكن التوصية

باستخدام مقياس SPR في المنهجيات التي تعتمد طبقات متعددة كما هو الحال في الإطار المقترح. يوضح العمود الأخير من الجدول الكسب الحاصل بتطبيق مقياس SPR بمعنى أنه يشير إلى كم نقطة مئوية يتجاوز فيها مقياس SPR مقياس EPR عند تفعيل V2V Cache حيث يظهر أن EPR يخفي ما بين 0 إلى 31.5 نقطة مئوية ويزداد هذا الفرق مع زيادة كثافة المركبات.

الخلاصة:

قدمنا في هذا البحث إطاراً متكاملاً لإدارة الثقة في شبكات VANETs باستخدام سلاسل الكتل المستضافة في السحابة بهدف منع التلاعب والتعديل. يعتمد الإطار المقترح على ثلاث ركائز أساسية وهي: أولاً الفصل بين هوية وثقة المركبات وثانياً توظيف ذاكرة مؤقتة داخل المركبات V2V Cache مبنية على مرشح Bloom وثالثاً تخفيف الضغط على السحابة التي تستضيف سلسلة الكتل وتخزن بداخلها قرارات الثقة لكل مركبة.

أثبتت نتائج التجارب كفاءة استخدام V2V Cache حيث بلغت نسبة إصابة الكاش 98.8% الأمر الذي خفف الحمل عن السحابة بنسبة 49% إلى 74% وهذه النسبة متعلقة بكثافة المركبات في الشبكة وبالتالي يمكن القول بأن هذا الإطار مناسب في البيئات ذات الكثافات المرورية العالية. تم تحسين نسبة تسليم الرزم بوجود الكاش وتزداد هذه النسبة بزيادة عدد المركبات.

أظهرت نتائج التجارب حسب مقياس Recall أن وجود معلومات الثقة لدى المركبات ساهم في تحسين قدرة النظام على الكشف. تبين من خلال البحث قصور المقياس EPR الذي يركز على المنع على مستوى السحابة متجاهلاً المنع عبر V2V Cache الأمر الذي دفعنا لتعريف مقياس SPR الذي يجمع المنع على مستوى المركبات والسحابة. أظهر المقياس قدرة النظام على المنع بنسبة 82%-100% مقارنة بمقياس EPR الذي وصلت فيه النسبة 60%-100%. كشفت النتائج عن تحدي

يتمثل بمعلومات الكاش القديمة نتيجة تأخر التحديث وهو ما ظهر كانهخفاض في EPR في سيناريو 60 مركبة.

الآفاق المستقبلية:

يتيح لنا هذا البحث عدة آفاق لأعمال بحثية مستقبلية تتمثل بتعديل زمن صلاحية الكاش بشكل تكيفي حسب كثافة الشبكة ومعدل المنع في الشبكة لتخفيف أثر البيانات القديمة. كما يمكن أيضاً العمل على آلية لتحديث كاش المركبات بشكل فوري بدل الانتظار الدوري لعملية التحديث. تعزيز الخصوصية من خلال تقنيات متقدمة مثل Group Signatures و Ring Signatures و Zero Knowledge-Proof للتحقق من الهوية.

المراجع:

- [1] M. Razafimanjato, M. Saad, and D. Kim, "Blockchain-based trust management systems in the Internet of Vehicles: A comprehensive survey," ICT Express, 2025.
- [2] H. Liu, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in VANETs," Journal of Parallel and Distributed Computing, vol. 151, pp. 61–69, 2021.

- [3] E. Memary, C.-C. Shen, H. Guo, and M. M. Nejad, "TrCoin: A blockchain-based robust trust management system for VANET," *ACM Journal on Autonomous Transportation Systems*, vol. 2, pp. 1–20, Apr. 2025.
- [4] C. Pu, "Blockchain-based trust management using multi-criteria decision-making model for VANETs," *TechRxiv*, 2020.
- [5] F. Ghovanlooy Ghajar, J. Salimi Sratakhti, and A. Sikora, "SBTMS: Scalable blockchain trust management system for VANET," *Applied Sciences*, vol. 11, no. 24, p. 11947, 2021.
- [6] W. Ruan, J. Liu, Y. Chen, S. M. N. Islam, and M. Alam, "A double-layer blockchain based trust management model for secure Internet of Vehicles," *Sensors*, vol. 23, no. 10, p. 4699, 2023.
- [7] E. Memary, C.-C. Shen, H. Guo, and M. M. Nejad, "Blockchain and deep learning based trust management for Internet of Vehicles," *Simulation Modelling Practice and Theory*, vol. 118, p. 102555, 2022.
- [8] W. Ahmed, D. Wu, and D. Mukathe, "Blockchain-assisted privacy-preserving and context-aware trust management framework for secure communications in VANETs," *Sensors*, vol. 23, no. 12, p. 5766, 2023.

- [9] E. Khatibi and M. Sharifi, "BusCache: V2V-based infrastructure-free content dissemination system for Internet of Vehicles," Vehicular Communications, vol. 46, p. 100746, Apr. 2024.
- [10] R. Tahir et al., "Blockchain enabled privacy provisioning scheme for location based services in VANETs," PLOS ONE, 2025.
- [11] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J.-P. Hubaux, "Certificate revocation in vehicular networks," LCA Tech. Rep., EPFL, 2006.
- [12] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom Filters," ICT Express, vol. 3, no. 3, pp. 100–103, 2017.
- [13] G. Samara, W. A. H. Al-Salihi, and R. Sures, "Design of simple and efficient revocation list distribution in urban areas for VANETs," in Proc. 2nd Intl. Conf. on Network Applications, Protocols and Services (NETAPPS), 2010.
- [14] X. Guo, J. Lin, Z. Wu, and Y. Guan, "Improving efficiency of pseudonym revocation in VANET using Cuckoo Filter," in Proc. IEEE VTC-Fall, 2020, pp. 1–5.
- [15] M. Khodaei and P. Papadimitratos, "Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in VANETs," in Proc. ACM WiSec, 2018, pp. 172–183.

