أثر سرعة العربة في حماية خصوصية موقع العربات في شبكات VANET

م. ازدهار شاليش
كلية هندسة تكنولوجيا المعلومات والاتصالات، جامعة طرطوس، طرطوس، سورية.
Eng.ezdharshalessh@gmail.com

المُلخَّص
تم تصميم شبكات VANET للتخفيف من حوادث المرور بالإضافة إلى إعلام السائقين بحالة الطرق، وذلك من خلال إرسال رسائل beacons فيما بينها، إمكانية التصنت على رسائل beacons متاح بسبب الوسط اللاسلكي ، هذا الأمر سبب بعض المخاوف لدى السائقين بسبب إمكانية تعقب العربة. تم في هذا البحث دراسة المقارنة بين استخدام إستراتيجية تجميع العربات وفقاً لسرعتها ضمن منطقة العمل Work Zoneو بين إستراتيجية SLOW بحالتي 30km/h & 40km/h.
تمت محاكاة الشبكة باستخدام SUMO و OMNET++ و Veins.تظهر نتائج المحاكاة إن Work Zone أكثر فعالية من ناحية تحسين مستوى الخصوصية و تقليل التعقب مقارنة بإستراتيجية SLOW.

Abstract
Designed VANET networks to reduce traffic accidents as well as to inform the drivers state of the roads, so by sending beacons messages between them. the possibility of eavesdropping these messages is available because of the wireless medium, this caused some concerns for drivers because of the possibility of tracking the vehicle. In this paper, a comparison study was made between the use of the vehicle assembly strategy according to its speed within the Work Zone and the SLOW strategy of 30km / h & 40km / h.The network is simulated using SUMO, OMNET ++ and Veins. Simulation results show that Work Zone is more effective in terms of improving privacy and reducing tracking compared to SLOW strategy.

1. مقدّمة
أن هدف شبكات VANET بالدرجة الأولى تأمين السلامة على الطرق ، من خلال رسائل دورية تسمى beacons إلا إنها تصبح غير مرغوبة عندما يتم إهمال الخصوصية[1] . تبث رسالة beacon عبر قناة التحكم (DSRC control channel) بتردد يتراوح من 1 إلى 10 هرتز كما هو مقترح من قبل الهيئات المعيارية مثل IEEE و ETSI و SAE[2].
تتضمن رسائل السلامة معلومات حساسة عن الحالة الراهنة للمركبات مثل مواقعها ،سرعاتها ،اتجاهها. يقوم سائق العربة بتسجيل العربة لدى الهيئة الموثوقة التي تزود السائق بمعرف فريد للعربة ، بالإضافة إلى عدة أسماء مستعارة متواجدة ضمن OBU . تستخدم العربة عند إرسال رسالة beacon اسماً مستعاراً ، لكل اسم مستعار زمن حياة، عند انتهاء صلاحية الاسم المستعار ، تقوم العربة باستبداله وهذا المتطلب الأول لحماية الخصوصية . المتطلب الثاني لحماية الخصوصية : يجب أن تكون الخصوصية شرطية أي تعد الهيئة الموثوقة هي الوحيدة التي تعلم بالعلاقة بين الأسماء المستعارة و الهوية الحقيقة للعربة .
الحد الأدنى من الإفصاح هو المتطلب الثالث للخصوصية، أي يجب أن تقتصر كمية المعلومات التي يكشف عنها المستخدم على المعلومات الضرورية لضمان وظائف VANET. يجب عدم الربط بين رسالتين تابعتين لنفس العربة لمدة طويلة و هو المتطلب الأخير للخصوصية.

2. هدف البحث
هدف البحث المقارنة بين استراتيجية SLOW القائمة على الصمت الراديوي عند سرعات محددة مسبقاً و بين استراتيجية تجميع العربات اعتماداً على سرعاتها ، وذلك ضد المهاجم السلبي العام global passive adversary وقياس بارامترات الخصوصية (عدد مرات إرباك المهاجم والانتروبيا و حجم مجموعة إخفاء الهوية)بالإضافة إلى بارامترات التعقب (نسبة المئوية لزمن التعقب المستمر).

3. أدوات البحث

تم إجراء المحاكاة باستخدام Veins عبارة عن إطار محاكاة اتصال بين العربات يعتمد على نموذج محاكاة ثنائي الاتجاه و له دخلين هما OMNET++ برنامج محاكاة الشبكة القائم على الحدث (Objective Modular Network Test bed in C++) وSUMO(Simulation of Urban Mobility)برنامج محاكاة حركة المرور على الطريق و سبب اختيار Veins هو قدرته على محاكاة طبقات الشبكة الكاملة 802.11P، IEEE 1609.4 DSRC / WAVE .

4. الدراسات المرجعية

تم طرح فكرة استخدام التوقيع الدائري Ring Signature للمصادقة و توقيع رسالة beacon بهدف توفير إمكانية المحافظة على خصوصية الموقع للعربة ،وتمت دراسة هذا النظام بشكل تحليلي و أظهر فعاليته في إخفاء الهوية [3] ،ولكنه يحتاج إلى زمن معالجة أعلى مقارنة بنظم مصادقة المفتاح العام.

تم تطوير استراتيجية Mix context [4]،وذلك بإضافة السرعة ،المسافة بين العربات ،id للطريق و لذلك سميت بإستراتيجية Mix context Enhanced، قد تبقى العربة تسير لفترة زمنية معينة بدون أن تجد عربة مجاورة لها ،أو لها نفس السرعة أو الاتجاه ،يحدث مثل هذا الأمر عادة عند قيادة العربة ليلاً في الطرق السريعة[5] .

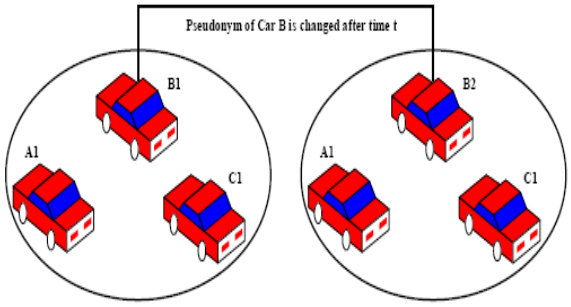
تم استغلال وجود أماكن عامة(على سبيل المثال مراكز التسوق ، مطاعم ، كراج للعربات) ضمن المدينة أو منطقة جغرافية معينة والتي سميت بالبقع الاجتماعية لإنشاء استراتيجية

PCS: Pseudonym Changing at Social Spots ،تقوم بحماية خصوصية موقع العربة عند تواجدها في مثل هذه البقع الاجتماعية . افتراض الباحثون أن إشارة المرور الحمراء تشكل بقعة اجتماعية صغيرة على اعتبار أن العربات تتوقف لفترة قصيرة وثابتة من الزمن ،تمت دراسة هذه الإستراتيجية بإدخال

KPSD: key-insulated pseudonym self-delegation،حيث تقوم الهيئة الموثوقة بتقديم مفتاح مميز لمالك العربة [6]. لكن في حال كانت Social Spot كبيرة مثل مراكز التسوق ،فإن العربات ستبقى لفترة طويلة و ستغادر البقعة الاجتماعية عشوائياً .وهنالك احتمال لهجوم الربط كما هو موضح بالجدول (1) و الشكل (1).

جدول 1: هجوم الربط [6]

S.No	Vehicles	Pseudo id at SP	Pseudo id after t1	Pseudo id after t2	Pseudo id after t3
1	A	0011	0011	0011	0011
2	B	0012	0012	0018	-
3	C	0013	0016	-	-
4	D	0014	0014	0014	0019
5	E	0015	0017	-	-



شكل 1 . هجوم الربط النحوي [6]

تقوم العربة بتغير اسمها المستعار في منطقة مزج مشفرة يتم إنشائها ديناميكاً
DMLP:Dynamic mix-zone for location privacy in vehicular networks. تتطلب هذه الإستراتيجية توزيع عدد كافي من RSU بحيث تغطي كامل الشبكة ، بالإضافة إلى حاجتها لزمن معالجة إضافي ناتج عن بث العربة لرسالة طلب إنشاء منطقة مزج ،الزمن اللازم لإرسال المفتاح المتناظر لها و لجيرانها في حال تواجدهم . بما أن شبكات VANET تتميز بحركية عالية ، الأمر الذي يتطلب تحكم إضافي لإنشاء المنطقة و توزيع المفتاح قبل مغادرة العربة للمنطقة[7] .

5. نموذج الشبكة المدروس

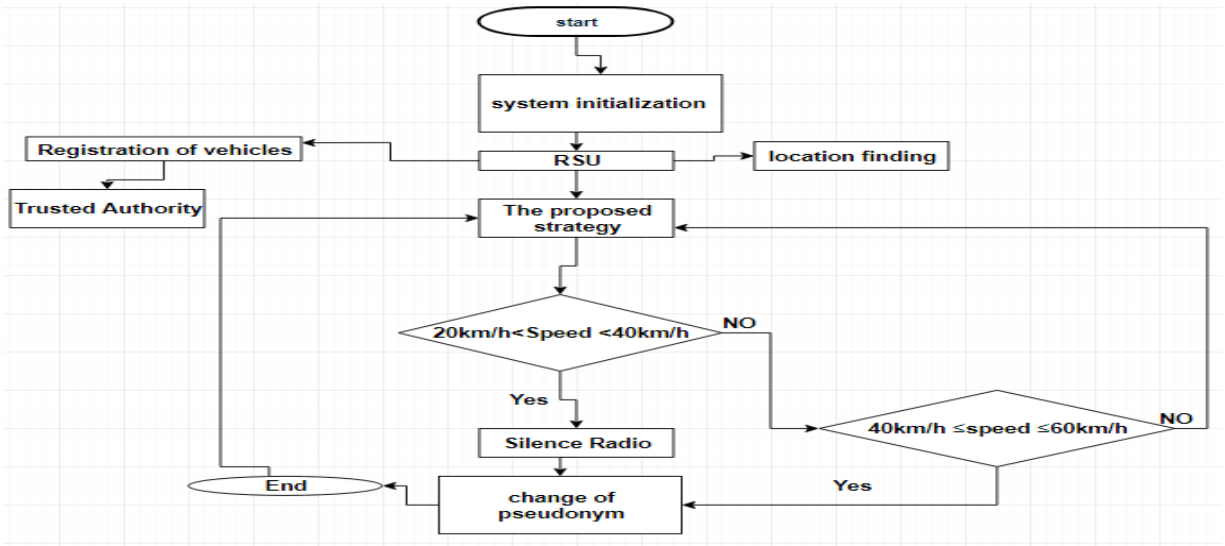
تتكون الشبكة من مجموعة من العربات ، حيث يتم تجهيز كل عربة بجهاز
OBU: On-Board Unit، يسمح للعربة بالتواصل مع العربات الأخرى. تتضمن كل عربة نظام GPS:Global Positioning System ، المكون من جهاز استقبال GPS وخريطة رقمية. يسمح هذا النظام بالحصول على الموقع ،الوقت الحالي ،معرف مقطع الطريق R_{id} الذي تسير عليه العربة. تقوم كل عربة بشكل دوري ببث رسالة سلامة كل t ميلي ثانية .
تسجل كل عربة لدى CA:Certification Authority قبل انضمامها إلى شبكة VANET. أثناء التسجيل ، يتم تحميل كل عربة V_i مسبقًا بمجموعة m من الأسماء المستعارة وهي مفاتيح عامة معتمدة من CA. لكل اسم مستعار من مجموعة الأسماء المستعارة لعربة V_i شهادة يتم تقديمها من قبل CA، و يتم توقيع رسائل السلامة بشكل صحيح بواسطة المفتاح الخاص الموافق للاسم مستعار لضمان المصادقة. يتم إرفاق الشهادة بكل رسالة لتمكين العربات الأخرى من التحقق من صحة المرسل[8].

6. نموذج المهاجم المدروس

تم الاهتمام بدراسة حماية خصوصية الموقع ضد نموذج المهاجم السلبي العام global passive adversary.حيث يهدف المهاجم إلى تعقب العربة المستهدفة عن طريق التصنت على جميع اتصالات أي عربة داخل منطقة الاهتمام ، نموذج المهاجم يدرك نموذج الشبكة و التقنية المستخدمة لحماية خصوصية الموقع .

7. استراتيجية حماية خصوصية موقع العربة

تم تطبيق ثلاث سيناريوهات لحماية خصوصية موقع العربة
السيناريو الأول :تطبيق استراتيجية تجميع العربات اعتماداً على سرعتها في منطقة العمل Work Zone كما في الشكل (2).

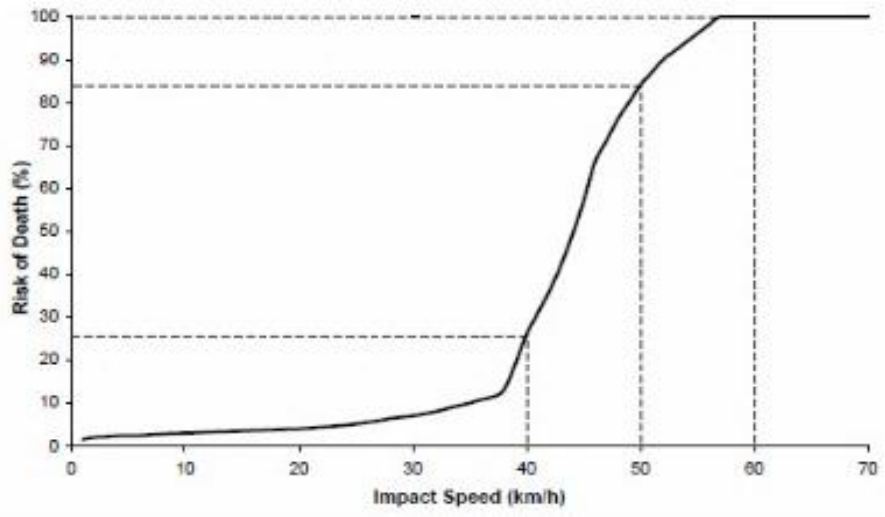


شكل 2 سيناريو تطبيق استراتيجية تجميع العربات اعتماداً على سرعتها في منطقة العملWork Zone .

يتم تجميع العربات اعتماداً على سرعتها ، وتم تصنيف السرعات إلى مجموعتين:

المجموعة الأولى : السرعات المنخفضة بين [20KM/H,40KM/H]

يمثل الشكل (3) العلاقة بين زيادة سرعة العربة و النسبة المئوية لخطر الوفاة ، كلما زادت سرعة العربة كلما كانت النسبة المئوية لخطر الوفاة أعلى ،بالتالي عندما تكون سرعة العربة ضمن المجال [20km/h -40km/h] تكون النسبة المئوية لخطر الوفاة أقل من [9]30% ، لذلك تم اختيار هذه المجموعة لدخول العربة بحالة صمت راديوي عند مغادرتها لمنطقة المزج .



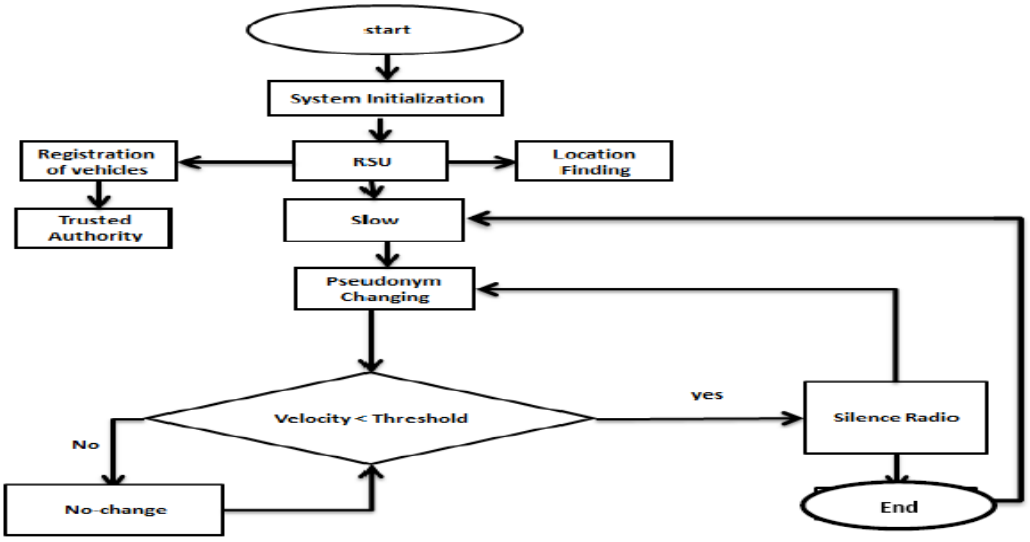
شكل 3 خطر الوفاة وفقاً لسرعة العربة[9]

المجموعة الثانية : السرعات المتوسطة [40KM/H,60KM/H]

هنا عندما تجد العربة أن سرعتها ضمن هذا المجال تقوم بتغير اسمها المستعار .

عملية تجميع العربات اعتماداً على سرعتها ، لتحقيق مزج أعلى عند تغير الاسم المستعار ،بالتالي إرباك المهاجم .

السيناريو الثاني: تطبيق استراتيجية SLOW الموضحة بالشكل (4) .



شكل 4 خوارزمية SLOW

العربة هنا تبقى بحالة فحص دائم لسرعتها وعندما تصبح سرعتها أقل من العتبة ،تدخل حالة صمت راديوي ثم تقوم بعملية تغيير اسمها المستعار .

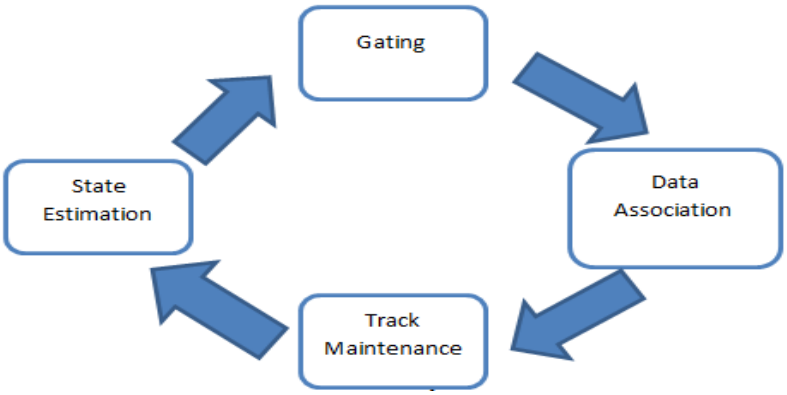
تمت دراسة حالتين لعتبة السرعة :

1- عتبة السرعة أقل أو يساوي 30km/h.

1- عتبة السرعة أقل أو يساوي 40km/h

7- خوارزمية التعقب المستخدمة

تم استخدام خوارزمية التتبع NNPDA: Nearest Neighbor Probabilistic Data Association المقترحة في [10] و ذلك لفعاليتها في تتبع رسائل beacons مجهولة المصدر مع كثافة عربات مختلفة و الموضحة بالشكل (5) .



الشكل (5) آلية التتبع [10]

تتكون خوارزمية التتبع من أربع مراحل متكررة على النحو التالي:

1- تخمين الحالة باستخدام مرشح Kalman الذي يستخدم للحصول على حالة دقيقة للمركبات باستخدام قياسات غير دقيقة مكتسبة من beacon،وحالات تخمين تم الحصول عليها من نموذج Kinematic model محدد مسبقا.

2- يتم تنفيذ مرحلة Gating قبل مرحلة اقتران البيانات لمنع الحسابات غير الضرورية ،أي حذف التكرارات الناتجة عن وصول رسالة beacon واحدة من أكثر من متصنت .

3- اقتران البيانات عن طريق ربط كل رسالة beacon مع العربة التي نشأت منها .

يتم تطبيق هذه المرحلة فقط عند وجود منارة واحدة أو أكثر تتضمن أسماء مستعارة جديدة ومسار واحد أو أكثر غير مخصص ل beacon باستخدام مطابقة اسم مستعار. خلاف ذلك ، يتم ربط beacons المتتالية عن طريق مطابقة الأسماء المستعارة المتشابهة.

4- هناك حاجة إلى مرحلة صيانة المسار للتعامل مع بدء المسار ،التأكيد ،الحذف لأن عدد العربات هو ديناميكي.

8. مقاييس الخصوصية و التعقب

1.8 حجم مجموعة عدم الكشف عن الهوية Anonymity set size

مجموعة عدم الكشف عن الهوية Anonymity set المشار إليها بـ AS ، هي مجموعة من العربات التي لا يمكن تمييزها عن الهدف مع المجموعة المتضمنة الهدف نفسه،و العلاقة (1) تمثل متوسط حجم مجموعة إخفاء الهوية الأعظم أثناء التتبع ، حيث يمثل nVeh عدد العربات التي تم تعقبها [11] .

$$\text{Average max AS size per trace} = \frac{\text{meanMaxASS}}{\text{nVeh}} (1) \qquad (1)$$

2.8 الانتروبيا لحجم مجموعة عدم الكشف عن الهوية Entropy of the anonymity set size

الانتروبيا تمثل أحد مفاهيم نظرية المعلومات التي تعبر عن عدم اليقين في متغير عشوائي. وعلى النقيض من حجم مجموعة عدم الكشف عن الهوية anonymity set size ، فإن الانتروبيا لحجم مجموعة عدم الكشف عن الهوية ، والتي يرمز إليها H_p ، تسمح بالتعبير عن معرفة الخصم لكل عربة في مجموعة عدم الكشف عن الهوية . يتم حساب الانتروبيا باستخدام الصيغة التالية:

$$H_p = -\sum_{i=1}^{|AS|} P_i log_2 P_i \qquad (2)$$

حيث يشير P_i إلى احتمال أن تكون العربة مستهدفة. إذا كانت جميع المركبات لها نفس الاحتمالية لتكون الهدف ، أي أن الاحتمالات موزعة بشكل موحد على مجموعة عدم الكشف عن الهوية ، تحقق الإنتروبيا عندها قيمة قصوى لها ، يرمز لها بـ H_{pmax} ، والتي تعطى بالعلاقة(3)[11].

$$\forall i: P_i = \frac{1}{|AS|}, H_{Pmax} = -\sum_{i=1}^{|AS|} P_i log_2 P_i = log_2 |AS| \qquad (3)$$

3.8 النسبة المئوية لزمن التتبع المستمر

تمثل أقصى فترة زمنية استطاع من خلالها المهاجم تتبع رسائل beacons لعربة ما دون أن يخطئ في تعين أحد رسائلها لعربة أخرى .

يوضح الشكل (6) مفهوم النسبة المئوية لزمن التتبع المستمر .

1- يمثل original vehicle trace مسار العربة Aلمدة 10 خطوات زمنية .

2- العربة A ستولد 10 رسائل beacons خلال 10 خطوات زمنية .

3- المهاجم يقوم بتتبع العربة A من خلال رسائل beacons الصادرة عنها .

4- يحصل المهاجم على رسالة beacon1 يحتفظ بمعلومات الرسالة من أجل استخدامها في هجوم ربط الأسماء المستعارة ، بعد مرور خطوة زمنية يحصل على رسالة beacon2 ، من خلال المعلومات الموجودة ضمنها يستطيع ربط هذه الرسالة مع العربة A وهكذا بالنسبة لـ beacon3.

5- عندما تصل رسالة beacon 4 إلى المهاجم ، يقوم المهاجم بتعينها للعربة B بشكل خاطئ و هكذا بالنسبة لرسالة beacon 5.

6- عندما تصل رسالة beacon6 ، يقوم بتعينها بشكل صحيح للعربة Aو هكذا بالنسبة لبقية رسائل beacons.

1- تكون أقصى فترة استطاع المهاجم أن يتتبع العربة دون أن يخطئ في تعين أحد رسائل العربة Aإلى العربة B هي (beacon6+beacon7+beacon8+beacon9+beacon10)مقسومة على الفترة الزمنية لتتبع العربة و بالتالي تكون النسبة المئوية لزمن التعقب المستمر هي 50%.تعطى علاقة النسبة المئوية لزمن التعقب المستمر[12] :

$$Continuous\ TrackingPercentage = \frac{\sum_v max_t l(t,v)}{\sum_v L(v)} \% \qquad (4)$$

حيث $l(t,v)$ طول الفترة الزمنية عندما يتم تعين تتبع العربة v إلى المسارt و $L(v)$ زمن حياة تتبع العربة v.

الشكل 6 حساب الحد الأقصى لماتريكس فترة التتبع المستمر لعربة واحدة

4.8 متوسط عدد مرات إرباك المهاجم

بما أن العربات تغير أسمائها المستعارة من أجل إرباك المهاجم وتجنب التتبع المستمر ، تم اقتراح مقياس لقياس ما يمكن لتقنية الخصوصية المقترحة تحقيق هذا الهدف.

يحدث الارتباك عندما يقوم المتعقب بتخصيص رسالة beacon لعربة ما لمسار ينتمي بالفعل إلى عربة أخرى ،أوعندما ينشئ المتعقب مسارًا جديدًا لرسالة beacons تابعة لعربة التي تمت مصادفتها سابقاً[11] .

تعطى علاقة متوسط عدد مرات إرباك المهاجم بالعلاقة :

$$C_{avg} = \frac{1}{N}\sum_{i}^{N}\sum_{k}^{L(v_i)} C_{i,k}\,, C_{i,k} = \begin{cases} 1 & T_{k-1}(v_i) \neq T_k(v_i) \\ 0 & otherwise \end{cases} \qquad (5)$$

حيث إن $T_k(v_i)$ المسار المخصص لرسالة beacon للعربة v_i في الخطوة الزمنية ,kN عدد العربات، $L(v_i)$ زمن حياة العربة .

والإرباك يحدث بحالتين هما : تغير الاسم المستعار أو فقدان رسالة beacon.

تحدث الحالة الأولى عندما يوجد العديد من رسائل beacons ذات أسماء مستعارة جديدة و معلومات مكانية مماثلة. الحالة الثانية تحدث عندما يتم فقدان رسالة beacon واحدة وتظهر رسالة beaconباسم مستعار جديد مع معلومات مكانية زمانية مماثلة بحيث يقوم المتعقب بتعيين هذا الرسالة إلى مسارمفقود. تحدث هذه الحالة الأخيرة في حال تم استخدام زمن عشوائي لإرسال رسالة beacon. ومع ذلك ، تحدث معظم الالتباسات بسبب حدوث تغييرات في الأسماء المستعارة و تزداد بزيادتها.

9. المحاكاة و مناقشة النتائج :

تم تطبيق استراتيجية حماية خصوصية موقع العربة في برنامج OMNET، باستخدام Veins الذي يقوم بإنشاء لكل عربة موجودة ضمن المنطقة المدروسة في SUMO عقدة لها في OMNET.

السيناريو الأول :استراتيجية تجميع العربات اعتماداً على سرعتها في منطقة العمل **Work Zone**

السيناريو الثاني :تطبيق خوارزمية SLOWبحالة 30KM/H.

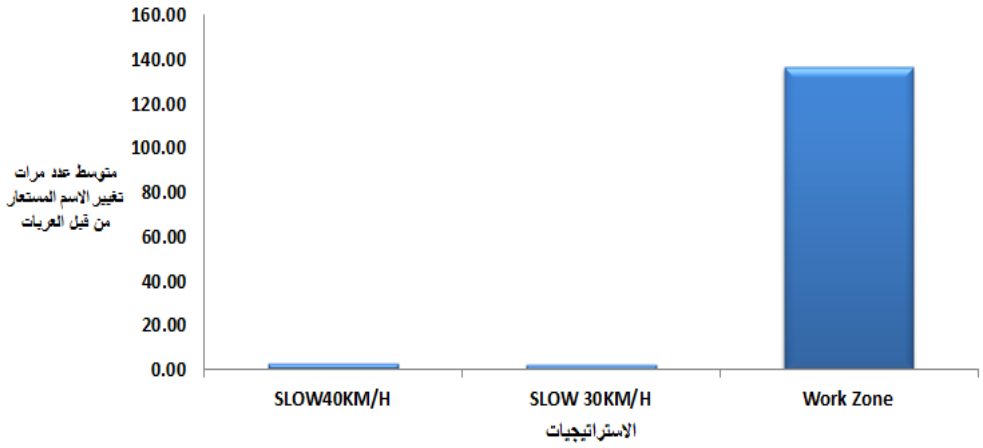
السيناريو الثالث: تطبيق خوارزمية SLOW بحالة 40km/h.

الجدول 2: يمثل بارامترات المحاكاة وفق المعيار IEEE 1609.4/802.11p[13]

Module	Parameter	Default Value
Veins	Transmission Power	20Mw
	Time of simulation	300s
	Bit Rate	18Mbps
	Thermal Noise	-110dBm
	Packet Header length	256bit
	Beacon Payload length	100 byte
	Beacon rate	1 HZ
Tracker	Eavesdropper Range	300m
	Eavesdropper overlap	30m
	Track Interval	1 s
الاستراتيجية المقترحة	Tracker.Max Silence	10s
	Number of vehicles	300
	Silent threshold	5s
السيناريو الأول: Work zone		
السيناريو الثاني SLOW 30KM/H	Threshold of velocity	30km/h
السيناريو الثالث SLOW 40KM/H	Threshold of velocity	40km/h

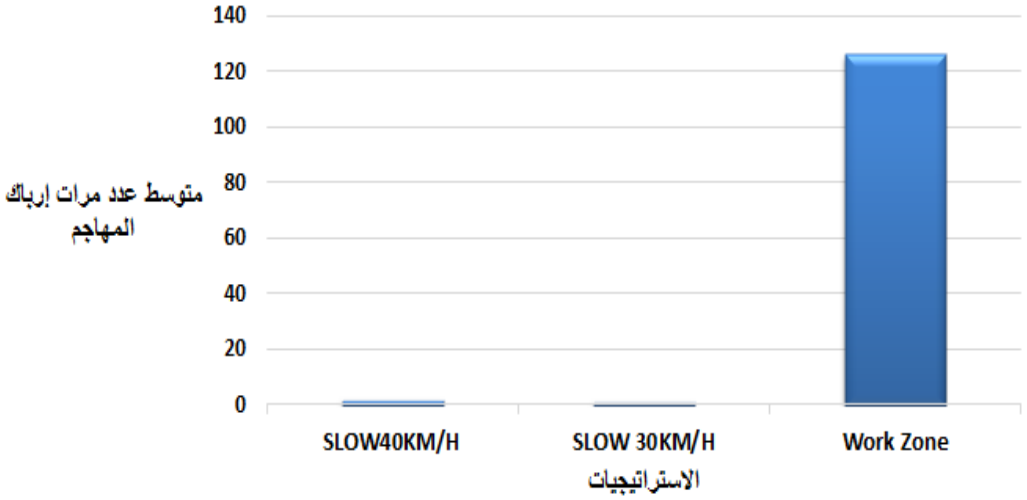
9. مناقشة النتائج

بما إن العربات في حالة سيناريو work zone ستبقى بحالة فحص دائم لسرعتها ،لذلك ستقوم بعملية تغيير اسمها المستعار بشكل دائم مما يؤدي إلى زيادة متوسط عدد مرات تغيير الاسم المستعار من قبل العربات كما في الشكل (7)، بالتالي زيادة الحمل على الشبكة بسبب حاجة العربات إلى التزود بأسماء مستعارة جديدة بشكل دائم .

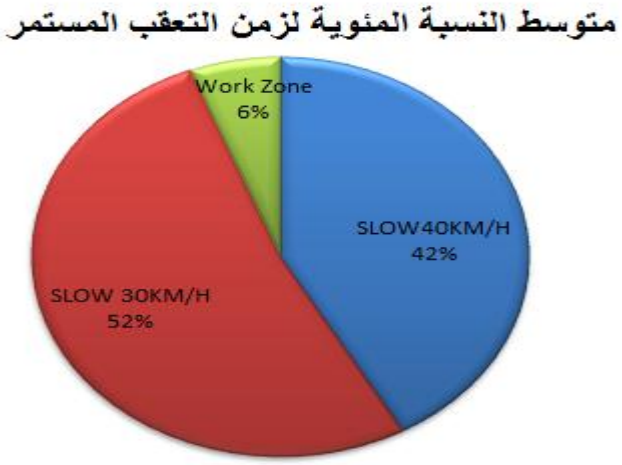


شكل 7 متوسط عدد مرات تغيير الاسم المستعار من قبل العربات .

زيادة متوسط عدد مرات تغيير الاسم المستعارمن قبل العربات ستؤدي إلى زيادة إرباك المهاجم كما في الشكل (8) ،وتقليل متوسط النسبة المئوية لزمن التعقب المستمر كما في الشكل (9).



شكل 8 متوسط عدد مرات إرباك المهاجم

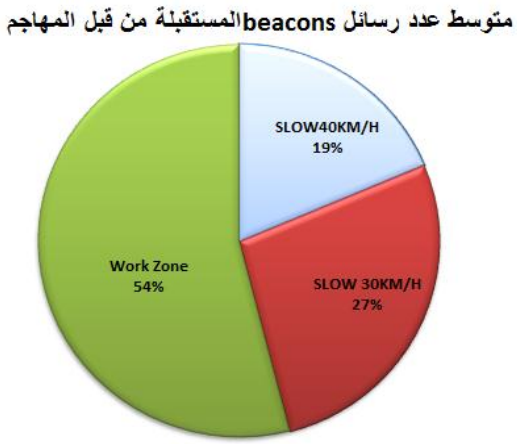


الشكل 9 متوسط النسبة المئوية لزمن التعقب المستمر .

مجموعة إخفاء الهوية بحالةWork Zone تمثل جميع العربات الموجودة داخل منطقة العمل ،أي أن متوسط حجم مجموعة إخفاء الهوية الأعظمي سيزداد بزيادة عدد العربات التي تقوم بتغيير اسمها المستعار كمافي الشكل (10) ، بالتالي زيادة متوسط الانتروبيا الأعظمية كما في الشكل (11) مقارنة بحالةSLOW30km/h &SLOW40km/h.

الشكل (10) متوسط حجم مجموعة إخفاء الهوية الأعظمي **الشكل (11) متوسط الانتروبيا الأعظمية**

احتمالية محافظة العربة على سرعة 40km/h أثناء مرورها بالمدينة و الطرق المزدحمة أعلى من احتمالية سيرها بسرعات عالية ،وبالتالي زيادة عدد مرات دخولها بصمت راديوي ولذلك سيقل متوسط عدد رسائل beacons المستقبلة من قبل المهاجم كما في الشكل (12).



الشكل (12)متوسط عدد رسائل beaconsالمستقبلة من قبل المهاجم

10. الاستنتاجات والتوصيات

تم تقييم أداء الإستراتيجية المقترحة لحماية الخصوصية بحالة Work Zoneلتغيير الاسم المستعار من قبل العربات اعتماداً على سرعتها بحالة السرعات المنخفضة تدخل العربات بحالة صمت راديوي ثم تقوم بتغيير أسمائها المستعارة ، بحالة السرعات المتوسطة فقط تقوم بتغيير أسمائها المستعارة ،ومقارنتها مع استراتيجية SLOWالقائمة على الصمت الراديوي فقط عند السرعات المنخفضة. أظهرت نتائج المحاكاة تحسين أداء Wok Zone من حيث متوسط الانتروبيا الأعظمية و متوسط حجم مجموعة إخفاء الهوية الأعظمية مقارنة مع Slow30km/H&Slow40km/H.

11. التوصيات المستقبلية :

تجدر الإشارة إلى إمكانية تحقيق تعاون بين العربات بما يساهم في حماية خصوصيتهم ،و ذلك من خلال التعاون داخل مناطق المزج و وفقاً لسرعتهم .

العربة تتعاون مع العربات المجاورة لها و الموجودة في منطقة المزج ذاتها ،لها سرعة مشابه لسرعتها ،لتغيير اسمائهم المستعارة معاً ،بالتالي سيرتبك المهاجم في معرفة العربة المستهدفة .

12. المراجع

[1] Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE communications surveys & tutorials, 13(4), 584-616.

[2] Doukha, Z., & Moussaoui, S. (2015). An sdma-based mechanism for accurate and efficient neighborhood-discovery link-layer service. IEEE Transactions on Vehicular Technology, 65(2), 603-613

[3] Mei, Y., Jiang, G., Zhang, W., & Cui, Y. (2014). A collaboratively hidden location privacy scheme for VANETs. International Journal of Distributed Sensor Networks, 10(3), 473151.

[4] Gerlach, M., & Guttler, F. (2007, April). Privacy in vanets using changing pseudonyms-ideal and real. In 2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring (pp. 2521-2525). IEEE.

[5] Liao, J., & Li, J. (2009, December). Effectively changing pseudonyms for privacy protection in vanets. In 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks (pp. 648-652). IEEE.

[6] Lu, R., Lin, X., Luan, T. H., Liang, X., & Shen, X. (2011). Pseudonym changing at social spots: An effective strategy for location privacy in vanets. IEEE transactions on vehicular technology, 61(1), 86-96.

[7] Ying, B., Makrakis, D., & Mouftah, H. T. (2013). Dynamic mix-zone for location privacy in vehicular networks. IEEE Communications Letters, 17(8), 1524-1527.

[8] Mansour, M. B., Salama, C., Mohamed, H. K., & Hammad, S. A. (2018). VANET Security and Privacy-An Overview. International Journal of Network Security & Its Applications (IJNSA) Vol, 10.

[9] Levulytė, L., Baranyai, D., Sokolovskij, E., & Török, Á. (2017). Pedestrians' role in road accidents. International Journal for Traffic and Transport Engineering, 7(3), 328-341.

[10] Emara, K., Woerndl, W., & Schlichter, J. (2013, June). Vehicle tracking using vehicular network beacons. In 2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 1-6). IEEE.

[11] Emara, K., Woerndl, W., & Schlichter, J. (2015, June). CAPS: Context-aware privacy scheme for VANET safety applications. In Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks (pp. 1-12).

[12] Emara, K., Woerndl, W., & Schlichter, J. (2013). Beacon-based vehicle tracking in vehicular ad-hoc networks.

[13] Ming, L., Zhao, G., Huang, M., Kuang, X., Zhang, J., Cao, H., & Xu, F. (2018, October). A General Testing Framework Based on Veins for Securing VANET Applications. In 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 2068-2073). IEEE.