مجلة جامعة طرطوس للبحوث والدراسات العلمية_ سلسلة العلوم الهندسية المجلد (٤) العدد (١) 2020
Tartous University Journal for Research and Scientific Studies- Engineering Sciences Series Vol. (4) No. (1) 2020

دراسة تأثير السرعة وعدد الجوار على أداء خوارزميات (Slow,CPN) في حماية خصوصية موقع العربات في شبكات VANET

*** علي أحمد أحمد**

**** ناجي ابراهيم محمد**

***** ازدهار شفيق شاليش**

(تاريخ الإيداع ١٧ / ٣ / ٢٠١٩ . قُبل للنشر ٢٧ / ٢ / ٢٠٢٠)

الملخّص

تم تصميم شبكات VANET للتخفيف من حوادث المرور إضافة إلى إعلام السائقين بحالة الطرق، وذلك من خلال ارسال رسائل beacons فيما بينها. إمكانية التنصت على رسائل beacons متاح بسبب الوسط اللاسلكي هذا الأمر سبب بعض المخاوف لدى السائقين بسبب إمكانية تعقب العربة و معرفة المواقع التي زارتها العربة، لذا يمكن استخدام هذا الأمر لتهديد أو لأجل الابتذال الشخصي. تمت دراسة تأثير زيادة السرعة في خوارزمية SLOW و زيادة المجال الراديوي للعربة وعدد الجوار في خوارزمية CPN. زيادة السرعة في خوارزمية SLOW زاد من مستوى الخصوصية ولكنه عانى من مسألة زيادة كمية استهلاك الاسماء المستعارة و التي تسبب حمل زائد على الشبكة . زيادة المجال الراديوي في خوارزمية CPN أعطى نتائج أفضل من ناحية الخصوصية بحالة وجود جار واحد على الأقل يرغب بتغير اسمه المستعار. باستخدام برامج المحاكاة ++OMNET و SUMO و VEINS.

الكلمات المفتاحية :خصوصية الموقع ، شبكات VANETs، الصمت الراديوي، سياق المزج، الأسماء المستعارة .

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

**مدرس، كلية هندسة تكنولوجيا المعلومات والاتصالات، قسم تكنولوجيا الاتصالات جامعة طرطوس، طرطوس، سورية.

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

مجلة جامعة طرطوس للبحوث والدراسات العلمية_ سلسلة العلوم الهندسية المجلد (٤) العدد (١) 2020
Tartous University Journal for Research and Scientific Studies- Engineering Sciences Series Vol. (4) No. (1) 2020

Study the effect of speed and number of neighborhood on the performance of the (Slow,CPN) algorithms in protect location privacy of vehicles in Vanets.

*** Ali Ahmad Ahmad**
**** Naji Ibrahim Mohammad**
***** Izdihar Chafick Chalich**

(Received 17 / 3 / 2019 . Accepted 27 / 2 / 2020)

Abstract

VANET Networks have been designed on the target of decreasing Traffic Accidents, besides acknowledging the drivers with the Road-Status by sending mutual beacons messages. The wireless milieu provides the possibility of tapping Beacons messages, what makes some worry among drivers, as the vehicle's location movement become revealed for others, so that pursuing it might be misused by those who exploit personal data to threaten them. The effect of speed increase in SLOW algorithm and increase of vehicle radio range and number of neighborhood in CPN algorithm were studied. Increasing speed in the SLOW algorithm increased the level of privacy, but suffered from the issue of increasing the amount of consumption of pseudonyms that cause overload on the network. Increasing the radio range in the CPN algorithm yields better privacy results if there is at least one neighbor who wants to change his pseudonym. Using simulations of OMNET ++, SUMO and VEINS.

Key Words: location privacy , VANETs networks ,radio silence, Mix-Context, Pseudonyms.

*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(Master), Department of Communication Technology, Faculty of Information and Communication Technology Engineering, Tartous University, Tartous, Syria

مقدّمة

على مدى العقد الماضي، جذبت شبكات VANET(Vehicular Ad-Hoc Networks) الكثير من الاهتمام من مجتمع الأبحاث وصناعة السيارات بسبب تأثيرها الكبير على أنظمة النقل الذكية ITS (Intelligent Transportation Systems) تم تطوير هذه التكنولوجيا في المقام الأول لتعزيز السلامة على الطرق وتوفير الكفاءة [1]. تسمح شبكات VANET للعربات بالتواصل فيما بينهاV2V (Vehicle-to-Vehicle)، وكذلك مع بنية تحتية مثبتةV2I (Vehicle-to-Infrastructure)، والتي تقدم مجموعة متنوعة من التطبيقات المثيرة للاهتمام. يمكن أن تتراوح هذه التطبيقات من التطبيقات المتعلقة بالسلامة ، مثل التحذير من الاصطدام وإعداد التقارير في حالات الطوارئ إلى التطبيقات غير الآمنة مثل المعلومات الترفيهية [2]. تعتمد لذلك، التطبيقات المتعلقة بالسلامة عادةً على المنارة beacon، أي يتم بث رسائل السلامة beacons بشكل دوري.

تسمى رسائل beacon رسائل التوعية التعاونية CAMs (Cooperative Awareness Messages) في أوروبا و رسائل السلامة الأساسيةBSM (Basic Safety Messages) في الولايات المتحدة [3] ويتم بثها عبر قناة التحكم DSRC control channel مع تردد عال يتراوح من 1 إلى 10 هرتز كما هو مقترح من قبل الهيئات المعيارية مثل IEEE و ETSI و SAE.

تتضمن رسائل السلامة معلومات حساسة عن الحالة الراهنة للعربات مثل مواقعها وسرعاتها[4]، الهدف من رسائل السلامة هو جعل العربات على دراية بالبيئة المحيطة بها ، الأمر الذي يحسن السلامة على الطرق. على سبيل المثال ، باستخدام هذه الرسائل ، يمكن للعربات أنّ تتوقع أو تكتشف مواقف خطرة يمكن أن تسبب أضراراً خطيرة على شبكات VANET مثل الاصطدامات والحوادث.

نتيجة لذلك ، يمكن للعربات اتخاذ قرارات لمنع مثل هذه العواقب السيئة. على الرغم من أن رسائل السلامة تكون مفيدة للسلامة على الطرق إلا أنها قد تستغل من قبل المهاجمين لتتبع المواقع غير المصرح بها للعربات [5]. وبسبب طبيعة الوسط اللاسلكي يمكن لمهاجم سلبي أن يتنصت بسهولة على جميع رسائل السلامة التي يتم بثها ضمن منطقة اهتمامه. ويمكنه بعد ذلك جمع رسائل السلامة وتحديد المواقع التي تمت زيارتها بواسطة العربات بمرور الوقت، الأمر الذي يشكل خطراً على حياة السائق لذلك تعد حماية خصوصية الموقع أمر بالغ الأهمية في نشر شبكةVANET .

أظهرت العديد من الدراسات التي أجريت لدراسة فعالية نهج تغيير الاسم المستعار أن التغيير البسيط للاسم المستعار غير فعال لتوفير المستوى المطلوب من حماية خصوصية الموقع لمستخدمي شبكة VANET.هذا يرجع إلى هجوم الربط بين الأسماء المستعارة وهناك نوعان من هذا الهجوم: الربط النحوي والربط الدلالي. وقد اقترحت العديد من استراتيجيات تغيير الاسم المستعار لتوفير الحماية ضد هذا الهجوم. الهدف من استراتيجية تغيير الاسم المستعار هو تحديد أين ومتى وكيف يجب على العربات تغيير أسمائها المستعارة لتوفير عدم إمكانية الربط بين الأسماء المستعارة .على الرغم من تنوع استراتيجيات تغيير الاسم المستعار الحالية فلا توجد استراتيجية مقترحة من الهيئات الدولية ليتم تطبيقها حتى الآن [6]. لمنع مثل هذه الهجمات تم اقتراح العديد من استراتيجيات تغيير الاسم المستعار. ويمكن تصنيف هذه الاستراتيجيات من حيث استخدام البنية التحتية إلى فئتين: استراتيجيات تغيير الاسم المستعار المعتمدة على البنية التحتية واستراتيجيات تغيير الاسم المستعار الموزعة. لا يمكن أن تعمل الاستراتيجيات القائمة على البنية التحتية دون دعم البنية التحتية. ويمكن اعتبار ذلك عيبًا لهذه الاستراتيجيات بسبب القيود المفروضة على

البنية الأساسية مثل تكاليف التطوير المرتفعة والتغطية المحدودة. لهذا السبب ، يكون الاعتماد على استراتيجيات تغيير اسم مستعار الموزعة على اعتبار إنها لا تتطلب أية مساعدة من البنية التحتية للعمل. يمكن أيضاً فرز استراتيجيات تغيير الاسم المستعار الموزعة الحالية من حيث كفاءتها لمنع هجومات ربط الأسماء المستعارة إلى ثلاث فئات:

(١) الاستراتيجيات التي تعتمد على آلية لمزامنة تغييرات الأسماء المستعارة بين العربات [7,8,9,10,11] تظهر هذه الاستراتيجيات ضعفها ضد المهاجم السلبي الذي يمكنه استخدام محتويات رسائل السلامة لربط الأسماء المستعارة. ويسمى هذا النوع من الهجوم بالربط الدلالي.

(٢) الاستراتيجيات التي تقترح تشفير رسائل السلامة في بعض الفترات الزمنية [١٢] يتم كسر هذه الاستراتيجيات بسبب وجود بعض المهاجمين السلبيين الداخليين الذين لديهم مفاتيح فك التشفير. لذا يتم الإفصاح عن محتويات رسائل السلامة إلى هؤلاء المهاجمين ، والتي يمكن أن توفر أيضاً دليلاً للمهاجم السلبي العام الخارجي لتنفيذ الربط الدلالي للأسماء المستعارة .

(٣) الاستراتيجيات التي تستخدم تقنية الصمت اللاسلكي [4,13,14] تُعدّ استراتيجيات هذه الفئة أكثر فعالية من الفئات السابقة لأنها يمكن أن توفر الحماية ضد كل من المهاجمين السلبيين الخارجيين والداخليين.

هدف البحث

تطرقنا إلى موضوع الخصوصية في شبكات VANET لما لها من أهمية في جعل هذه التقنية مقبولة من قبل عامة الناس بشرط المحافظة على خصوصية السائق و عدم معرفة المواقع التي يزورها ولهذا السبب كان هدف البحث دراسة تأثير زيادة السرعة و عدد الجوار في حماية خصوصية موقع السائق ضد هجوم الربط للأسماء المستعارة التي يقوم بها المهاجم و ذلك ضد المهاجم العام وقياس بارامترات الخصوصية (الانتروبيا و حجم مجموعة إخفاء الهوية (ASS) .

طرائق البحث و مواده

أُجريت المحاكاة باستخدام VEINS وهو 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 Testbed 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 .

متطلبات الخصوصية:

الخصوصية هي واحدة من حقوق الإنسان الهامة التي ينبغي حمايتها [١١]. ومع ذلك ، فإن التطور التكنولوجي الحالي يهدد هذا الحق ويقلل من سيطرة المستخدمين على المعلومات الخاصة بهم. لهذا السبب ، اقترح الباحثون مجموعة من المتطلبات لضمان حماية خصوصية مستخدمي هذه التقنيات. تم تحديد متطلبات الخصوصية الآتية لـ VANETs [11]:

- الحد الأدنى من الإفصاح Minimum disclosure: يجب أن تقتصر كمية المعلومات التي يكشف عنها المستخدم على المعلومات الضرورية لضمان وظائف VANET.

- عدم الكشف عن هويته Anonymity: يجب أن تكون الرسائل المرسلة من قبل عربة مجهولة ضمن مجموعة من العربات المحتملة. يتعارض هذا الشرط مع المساءلة accountability ، التي تعد أحد المتطلبات الأمنية الرئيسية لشبكة VANET. تنص المساءلة على أنه ينبغي أن تكون السلطات قادرة على تحديد أصل أية رسالة مرسلة. لهذا السبب ، يجب أن يكون إخفاء الهوية anonymity شرطياً في VANETs.
- عدم الارتباط unlink ability: لا يمكن الربط بين رسالتين تابعتين لنفس العربة لمدة طويلة.

من أجل تلبية هذه المتطلبات ، اقترح العديد من نظم المصادقة المجهولة anonymous authentication. ومنها مصادقة الاسم المستعار [9] و تم اعتمده من قبل كل من الأوساط الأكاديمية والصناعية [11]. والواقع أن المعايير الأمنية الحالية لمعيار IEEE 1609.2 [10] والمعايير ETSI 102941- v1.1.1 [10] تعتمد على بنية تحتية عامة تقليدية هي بنية المفتاح العام PKI(Public KEY infrastructure) ، حيث تقوم العربات بالتسجيل قبل انضمامها إلى شبكة VANET لدى CA (Certification Authority) و تحصل على مجموعة من المفاتيح العامة (الأسماء المستعارة) و المفتاح الخاص بالإضافة إلى شهادة خاصة بكل اسم مستعار . حيث يعد CA طرف موثوق في الشبكة و يُشغَّل من قبل منظمات حكومية تتوافق مع سياسات الخصوصية و تحافظ على العلاقة بين الأسماء المستعارة مع الهوية الحقيقية للعربات . تقوم كل عربة بتحديث اسمها المستعار بشكل متسلسل على فترات زمنية منتظمة و مستقلة عن العربات الأخرى ، مع العلم أن لكل اسم مستعار مدة صلاحية قصيرة لا يمكن إعادة استخدامه. علاوة على ذلك ، يجب أن يكون تغيير الاسم المستعار مصحوباً بتغيير جميع تعريفات طبقات الاتصالات مثل MAC وعناوين IP [13].

هجومات ربط الأسماء المستعارة

يمكن إجراء تعقب لمواقع العربة حتى مع تغيير الأسماء المستعارة بشكل متكرر. وذلك باستخدام هجوم ربط الأسماء المستعارة . هنالك نوعين من الهجومات [4]:

1 -هجوم الربط النحوي

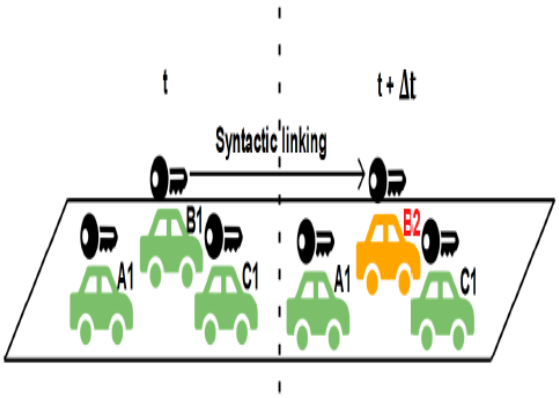
يوضح الشكل(1) الربط النحوي للأسماء المستعارة . على فرض أن العربة B فقط قامت بتغيير اسمها المستعار (من B1 إلى B2) خلال الفترة Δt بين العربات الثلاث التي تسير على الطريق. يمكن للمهاجم بسهولة الربط بين الأسماء المستعارة B1 و B2. و يمكن تنفيذ الحماية ضد هذا النوع من الهجوم من خلال استخدام آلية لمزامنة تغييرات الأسماء المستعارة بين العربات أي جعل عدد معين من العربات تقوم بتغير أسمائها المستعارة بنفس اللحظة .

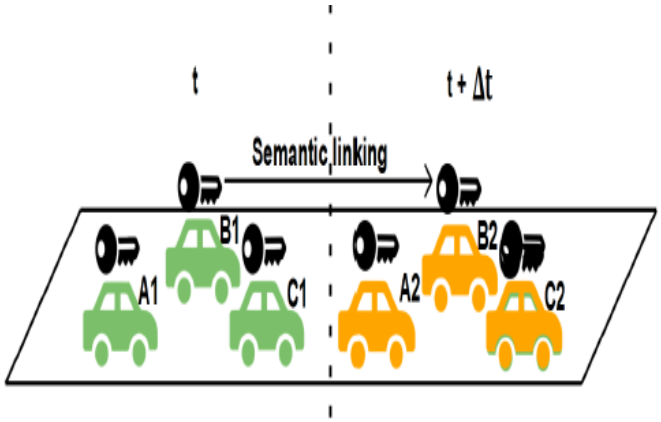
2 -هجوم الربط الدلالي :

يوضح الشكل(2) الربط الدلالي للأسماء المستعارة. يعد هذا الهجوم أقوى من هجوم الربط النحوي للأسماء المستعارة لأن المهاجم يعتمد على المعلومات المضمنة في رسائل السلامةbeacon لربط الأسماء المستعارة. على سبيل المثال ، يمكن للمهاجم التنبؤ بالموقع التالي للعربة باستخدام طريقة تتبع معينة [١٨]. وبناءً على هذا التنبؤ ، يمكن للمهاجم ربط الأسماء المستعارة B1 و B2 حتى إذا كانت المركبات الثلاث تغير اسمها

المستعار في نفس الوقت. لا يمكن القيام بالحماية من هذا النوع من الهجمات إلا من خلال منع المهاجم من الوصول إلى رسائل السلامة في بعض الفترات الزمنية أي استخدام استراتيجية الصمت الراديوي .

الشكل (1) :يمثل هجوم الربط النحوي **الشكل (2) :يمثل هجوم الربط الدلالي**





نموذج الشبكة المدروس

دُرِسَت شبكة VANET في مدينة ميونيخ بألمانيا . 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 ، المكون من جهاز استقبال GPS وخريطة رقمية. يسمح هذا النظام بالحصول على الموقع والوقت الحالي ومعرف مقطع الطريق R_{id}. تقوم كل عربة بشكل دوري ببث رسالة سلامة كل t ميلي ثانية ، حيث تتضمن كل رسالة موقع العربة و سرعتها بالإضافة إلى الزمن .قبل الانضمام إلى VANET ، تسجل كل عربة لدى CA (certification authority). 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.

نموذج المهاجم المدروس

نحن مهتمون بدراسة حماية خصوصية الموقع ضد نموذج المهاجم العالمي .حيث يهدف المهاجم إلى تعقب العربة المستهدفة عن طريق التنصت على جميع اتصالات أية عربة داخل منطقة الاهتمام ، و إن نموذج المهاجم يدرك نموذج الشبكة و التقنيات المستخدمة لحماية خصوصية الموقع .

1-أنواع المهاجمين في شبكة VANET [20]

- Global vs Local: بالمقارنة مع المهاجم المحلي ، يكون لدى المهاجم العام تغطية شاملة لـ VANET. ويمكنه بعد ذلك أن يتنصت على كل رسالة تنتشر عن طريق أية عربة .
- Active vs Passive: المهاجم النشط أكثر خطورة من المهاجم السلبي لأنه يمكن أن يغير أو يضخ الرسائل ، في حين أن المهاجم السلبي لا يمكنه سوى التنصت على الرسائل .
- Internal vs External: المهاجم الداخلي هو عضو مصادق في نظام VANETs. يُعدّ المهاجم الخارجي بمثابة متطفل مثل مراقب على البنية التحتية.

الخوارزميات المستخدمة لحماية خصوصية موقع العربة

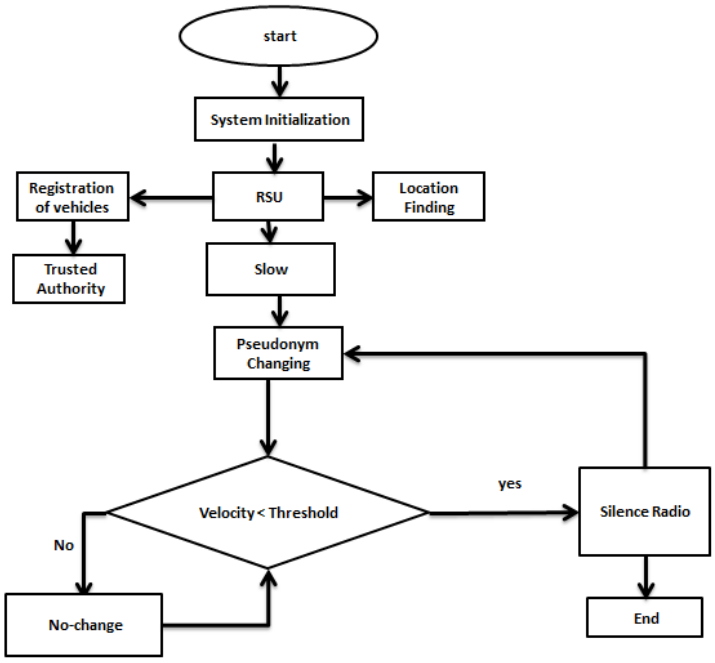
SLOW – 1

لا تحتاج هذه التقنية إلى أي تعاون صريح بين العربات أو إلى دعم من البنية التحتية .نفرض أن العربات لن تقوم بإرسال رسائل السلامة عندما تنخفض سرعتها إلى ما دون عتبة معينة لذلك سميت بهذا الاسم. وهذا يضمن بأن العربات التي تتوقف أو تتحرك ببطء في الازدحام سوف تمتنع عن نقل رسالة السلامة في هذه الفترة و ستقوم بتغيير اسمها المستعار في نفس الوقت و المكان مما يسبب إرباك المهاجم . السبب في اختيار سرعة معينة هي الفرضية القائلة بأن الحوادث المميتة تحدث بنسبة بسيطة جداً و نادرة، على اعتبار أن معظم العربات تخفف من سرعتها عند اجتيازها لتقاطع معين [18] .

مع فرض أن:

- عتبة السرعة هي 40km/h& 30 Km/h على اعتبار أن نسبة الحوادث الناتجة عن هذه السرعات هي 20% , 30% .
- و لن تبث العربة رسالة السلامة إذا كانت تسير بسرعة أقل من العتبة إلا إذا كان ذلك ضرورياً لأسباب تتعلق بأمن الحياة .
- اعُتبِرتَ إشارة المرور هي المكان الأفضل لتنفيذ استراتيجية SLOW. يوضح الشكل (3) خوارزمية Slow.

تقوم العربات الموجودة في الشبكة بطلب تزويدها بأسماء مستعارة عن طريق RSU التي تقوم بتسجيل تلك العربات لدى الطرف الثالث الموثوق الذي يملك الأسماء المستعارة ، تقوم العربات بتطبيق خوارزمية SLOW في حالة كانت سرعة العربة أقل من العتبة ثم تدخل فترة صمت راديوي (تتوقف العربات عن ارسال رسائل السلامة لفترة زمنية معينة) بعد ذلك تغير اسمها المستعار ، تبقى العربات بحالة فحص دائم لسرعتها .



الشكل (3) : يمثل خوارزمية SLOW.

2 -Cooperative Pseudonym Change (CPN)

بفرض العربات واقعة ضمن مسافة هي R ، ونعبر عن المنطقة المجاورة للعربة بـ NR_T وهي منطقة دائرية تتمركز في موقع العربة T مع نصف القطر R و تعد العربات الموجودة في المنطقة NR_T جيران لـ T.

تعتمد تقنية CPN على تغير الاسم المستعار اعتماداً على المحفز Trigger. حيث تقوم كل عربة بتحديث الاسم المستعار عندما تقابل trigger و بشكل عام يتكون trigger من عنصر واحد أو أكثر ، و يشير المكون إلى أي معلومات توفر إخفاء كافٍ فيما يتعلق بالمهاجم [21].

غالباً ما تتضمن المعلومات ما يلي : عدد جيران العربة و موقعها و السرعة و التسارع و الاتجاه و عمر الاسم المستعار . كلما زادت المكونات في trigger زادت صعوبة الربط بين الأسماء المستعارة السابقة و بين الأسماء المستعارة التالية . ومع ذلك فإن زيادة عدد المكونات يزيد من صعوبة مواجهة المحفز triggerأي نادراً ما تغير العربة اسمها المستعار ، بالنتيجة يكون لدى المهاجم زمن أكبر لمهاجمة العربة . إن الطريقة المستخدمة لرفع مستوى الخصوصية هي تمكين أكبر عدد ممكن من جيران العربة لتغير أسمائها المستعارة .

هكذا تعتمد مجموعة إخفاء الهوية للعربة بشكل رئيسي على عدد الجيران الذين يقومون بتغير أسمائهم المستعارة معها .و يتم تحديد عدد من الجيران ليقوموا بتغير أسمائهم المستعارة مع العربة بواسطة آلية trigger.

ومن الواضح أن أفضل نتيجة متوقعة عندما تغير العربة اسمها المستعار مع تغيير عدد معين من جيرانها لأسمائهم المستعارة و لتنفيذ التعاون يتم بث Ready Flag، حيث إن Ready Flagيعني :

1- إنها تقابل محفز trigger

2- تغير اسمها المستعار في slot التالي ، و تظهر عملية تنفيذ التعاون في slot كما في الخوارزمية (1).

الخوارزمية (1): تمثل آلية عمل CPN

```
1: Upon receiving beacons from neighbors in last slot
2: If (Ready flag is1) Then
3: Changes pseudonym
4: Ready flag=0
5: Else If (Any received beacon's Ready flag is 1) Then
6: Changes pseudonym
7: Else If (Meets a trigger) Then
8: Ready flag=1
9: End If
10: End If
11: End If
12: Broadcasts its beacon
```

عند استقبال رسائل من الجيران في آخر slot فإن العربة تفحص علم الجاهزية Ready Flag لعربات الجيران في حال كانت Ready Flag=1 تقوم العربة بتغيير اسمها المستعار و من ثم تصفر قيمة Ready Flag .

في حال عدم تحقق الشرط فتحقق ما إذا كانت تقابل المحفز trigger وإذا كان الأمر كذلك فسيتم تعيين Ready Flag=1 و هذا يعني إنها ستقوم بتغير اسمها المستعار في Slot التالي .

أي نلاحظ أن عملية التعاون تتم من خلال 2Slots متتاليين و على الرغم من تغير جيران العربة و لكن احتمال أن يكون جيران العربة خلال هذين 2slots متشابهين ، لكن في محاكاتنا لهذه التقنية نفترض أن جيران العربة لا يتغيرون قبل و بعد تغير الاسم المستعار .

يتمتع أسلوب التعاون هذا بخاصيتين :

١- لا يحتاج إلى مساعدة من البنية التحتية للطرق و بالتالي يمكن تطبيقه على اتصالات V2V ضمن شبكة VANET.

٢- يحتاج فقط إلى إدخال بت إضافي إلى رسالة Beacon .

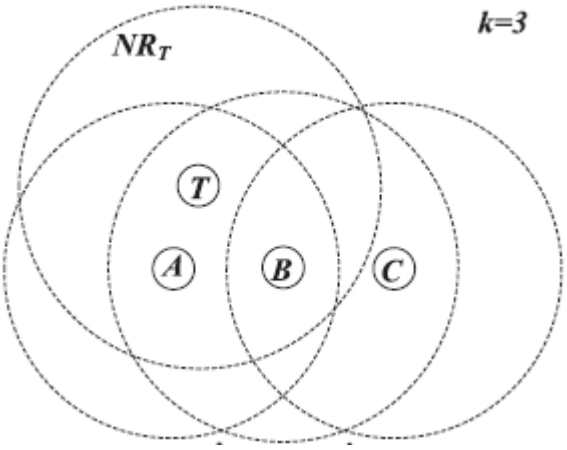
في الخوارزمية (1) نحن نأخذ عربة ما بشكل اعتباطي باعتبارها هي العربة المستهدفة T لدراسة تفاصيل التعاون على تغير الاسم المستعار و نشير إلى العربة V على إنها أحد جيران العربة T.الشكل (4) يوضح مجال تغطية العربة T و جيرانها الثلاث كل من (A,B,C). لنفترض أن العربة V هي واحدة من جيران العربة المستهدفة T و يجب أيضاً أن يكون T هو أحد جيران العربة V، سندرس حالات الأربع لتعاون بين V&T:

الحالة 1: عندما يكون علم الجاهزية Ready Flag للعربة T مساوي للصفر و Read Flag للعربة V مساوي للواحد ، يتم تمكين T لتغيير الاسم المستعار مع V في Slot التالي و بذلك يعتبر هذا السلوك هو سلوك تعاوني بينT مع V.

الحالة 2: عندما يكون Ready Flag للعربة T مساوي للواحد و Ready Flag للعربة V مساوي للصفر و بالتالي تستطيع العربة T أن تغير اسمها المستعار مع V في Slot التالي و بالتالي سلوك تعاوني Vمع T.

الحالة 3: عندما يكون Ready flag لكل من T,V مساوي للواحد ، و بالتالي لا يمكن اعتبار سلوك تغير الاسم المستعار هنا تعاوني كالتعاون بين Tو V لأن T أو V ستقوم بتغير اسمها المستعار و ذلك لأن Ready Flag=1 .

الحالة 4: عندما يكون Ready Flag لكل من Tو V مساوي للصفر فإن T,V كلاهما لا يقومان بتغير اسمائهم المستعارة في Slot التالي و بالتالي لا يوجد تعاون لأنه لا يحدث تغير للاسم المستعار .



الشكل (4) :يمثل مجال تغطية العربة T و جيرانها A,B,C

مقاييس الخصوصية و التعقب

1 –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 الأعظمي أثناء التتبع Average max AS size per trace، nVeh يمثل عدد العربات التي تم تعقبها [21].

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

2 –الانتروبيا لحجم مجموعة عدم الكشف عن الهوية Entropy of the anonymity set size:

الانتروبيا هي مفهوم قادم من 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 المهاجم 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)[21].

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

٣ –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 [21].

يوضح الشكل (٥) مفهوم النسبة المئوية لزمن التتبع المستمر .

١– يمثل original vehicle trace مسار العربة A لمدة ١٠ خطوات زمنية .

٢– العربة A ستولد ١٠ رسائل beacons خلال ١٠ خطوات زمنية .

٣– المهاجم يقوم بتتبع العربة A من خلال رسائل beacons الصادرة عنها .

٤– 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.

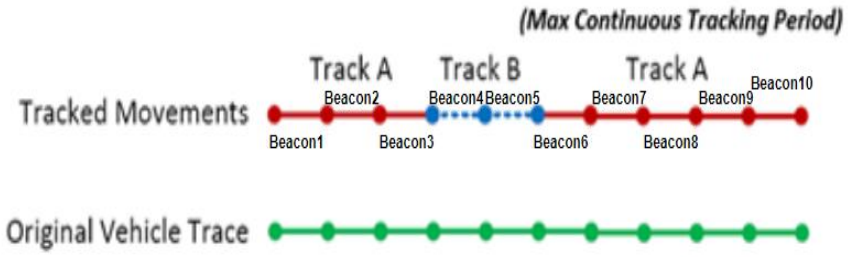
٥– عندما تصل رسالة beacon 4 إلى المهاجم ، يقوم المهاجم بتعينها للعربة B بشكل خاطئ و هكذا بالنسبة لرسالة beacon 5.

٦- عندما تصل رسالة beacon6 ، يقوم بتعينها بشكل صحيح للعربة A وهكذا بالنسبة لبقية رسائل beacons.

٧- 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[11] :

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

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



الشكل (٥) :يمثل حساب الحد الأقصى لفترة التتبع المستمر لعربة واحدة

٤- 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 أو عندما ينشئ المتعقب مساراً جديداً لرسالة beacons تابعة لعربة التي تمت مصادفتها سابقاً [11] ، تعطى علاقة متوسط عدد مرات إرباك المهاجم بالعلاقة :

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

حيث إن($T_k(v_i$ المسار المخصص لرسالة beacon للعربة v_i في الخطوة الزمنية N, k 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 beacon باسم مستعار جديد مع معلومات مكانية زمانية مماثلة بحيث يقوم المتعقب بتعيين هذا الرسالة إلى مسار مفقود. 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 .

المحاكاة و مناقشة النتائج :

يتم إجراء المحاكاة على مدينة ميونيخ الالمانية بمساحة 2.8KM*2.67KM كما هو موضح بالشكل (6) خريطة ميونيخ في برنامج SUMO.و عدد العربات الكلي هو ٣٠٠ عربة.

الشكل (6) : تمثل خريطة مدنية ميونيخ

الجدول (1):يمثل بارامترات المحاكاة

Module	Parameter	Default Value
Veins	Transmission Power	**20Mw**
	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**
SLOW	Speed threshold	**30km/h,40km/h**
	Silent threshold	**5s**
CPN	Radius	**100 m**
	Neighbors threshold	**1,2,4**

لقد تم إجراء عدة سيناريوهات مختلفة بوجود مهاجم عام و هي :

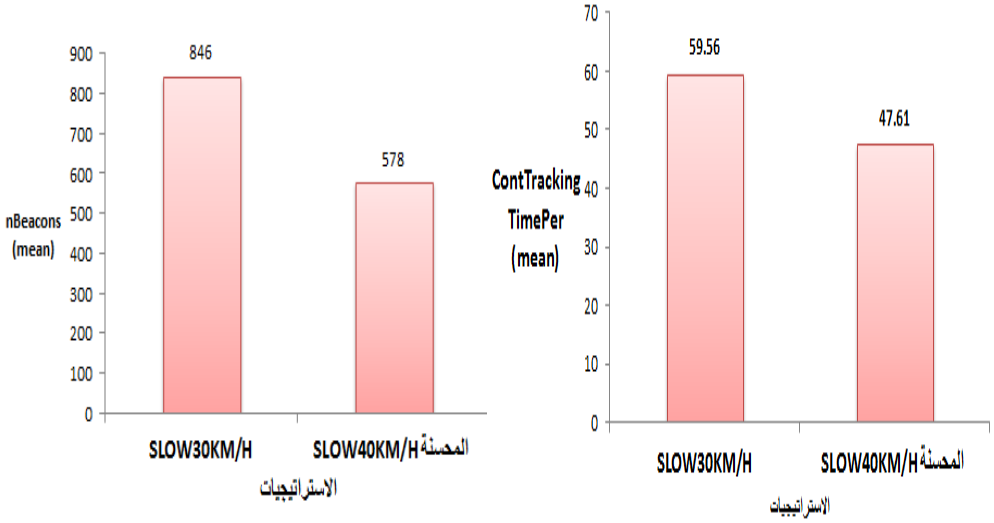
SLOW مع سرعة 30Km/h .

SLOW مع سرعة 40Km/h المحسنة.

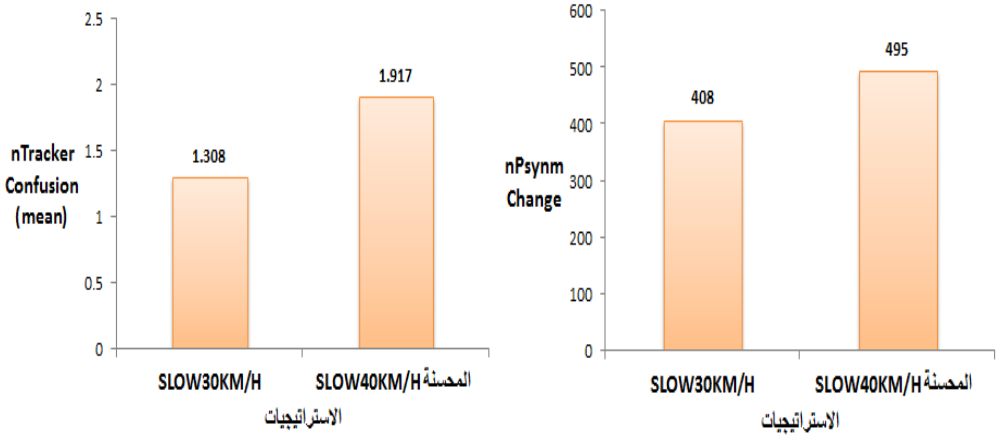
تطبيق خوارزمية CPN بحالة كان المجال الراديوي للعربة ٣٠ متر بحالة زيادة عدد جيران العربة.

تحسين خوارزمية CPN بحالة تم زيادة المجال الراديوي للعربة ١٠٠متر بحالة زيادة عدد جيران العربة .

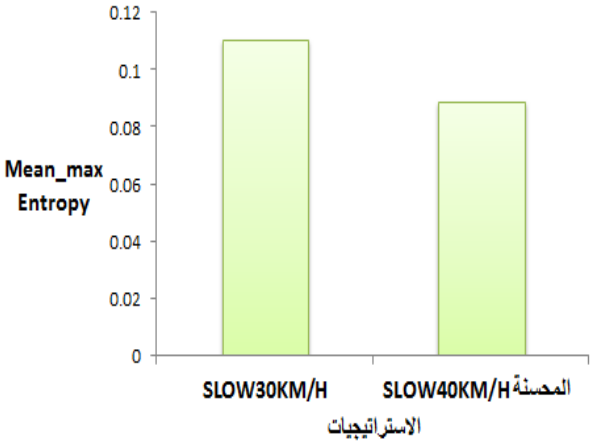
1- المقارنة بين SLOW30km/h و بين SLOW40km/h المحسنة



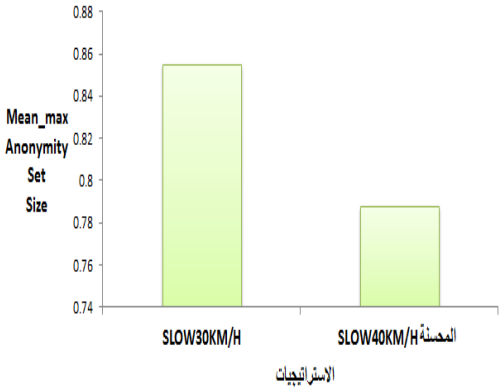
الشكل (٧): يمثل متوسط عدد رسائلBeacons المستقبلة من قبل المهاجم. الشكل (٨): يمثل متوسط النسبة المئوية لزمن التعقب المستمر



الشكل (٩) :يمثل عدد الأسماء المستعارة المتغيرة من قبل العربات الشكل (١٠): يمثل متوسط عدد مرات إرباك المهاجم



الشكل (١١) :يمثل متوسط الانتروبيا الأعظمية



الشكل (١٢): يمثل متوسط حجم مجموعة إخفاء الهوية الأعظمي

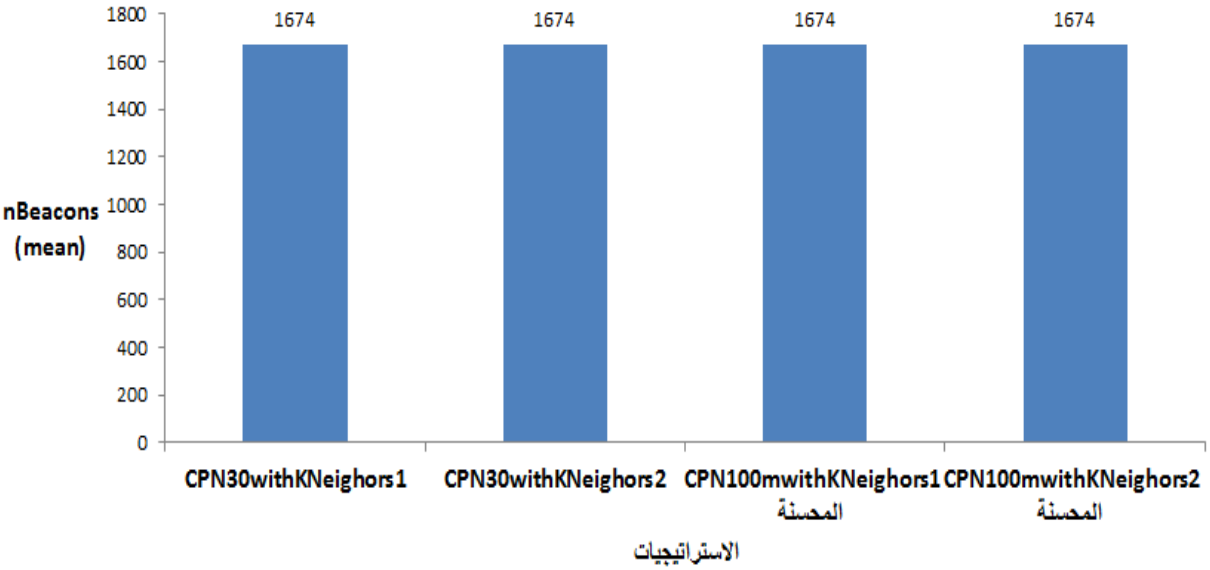
في استراتيجية SLOW بحالة السرعة 30km/h كانت عدد رسائل beacons المستقبلة من قبل المهاجم أعلى من عدد الرسائل المستقبلة بحالة 40KM/H و ذلك لأن احتمالية أن تحافظ العربة على سرعة 40km/h أعلى من احتمالية بقاء قيادتها بسرعة 30km/h و بالتالي لدى فحص العربة لسرعتها و إيجادها أقل من 40km/h ستدخل بحالة صمت راديوي لمدة 5ثواني ، تقوم بتغير اسمها المستعار و بالتالي سيزداد عدد مرات تغير الاسم المستعار من قبل العربات كما في الشكل (٩) و بالتالي زيادة الحمل على الشبكة، وعند انتهاء زمن الصمت ، تستيقظ لتعيد فحص سرعتها ، في حال بقيت 40km/h أيضاً ستدخل بحالة صمت راديوي وهكذا ، بالتالي عدد الرسائل المستقبلة من قبل المهاجم سيقل مقارنة بحالة 30km/h كما في الشكل (7).

بما أن العربة احتمالية أن تسير بسرعة 30km/h مرتبطة بحالة الطريق و بالتالي فإن متوسط النسبة المئوية لزمن التعقب المستمر يقل بزيادة عدد مرات دخول العربة بالصمت الراديوي و بالتالي المهاجم سيقوم بتعين خاطئ لرسائل beacons ، يكون متوسط النسبة المئوية لزمن التعقب المستمر بحالة SLOW40KM/Hأقل مقارنة مع SLOW30KM/H كما في الشكل (٨).

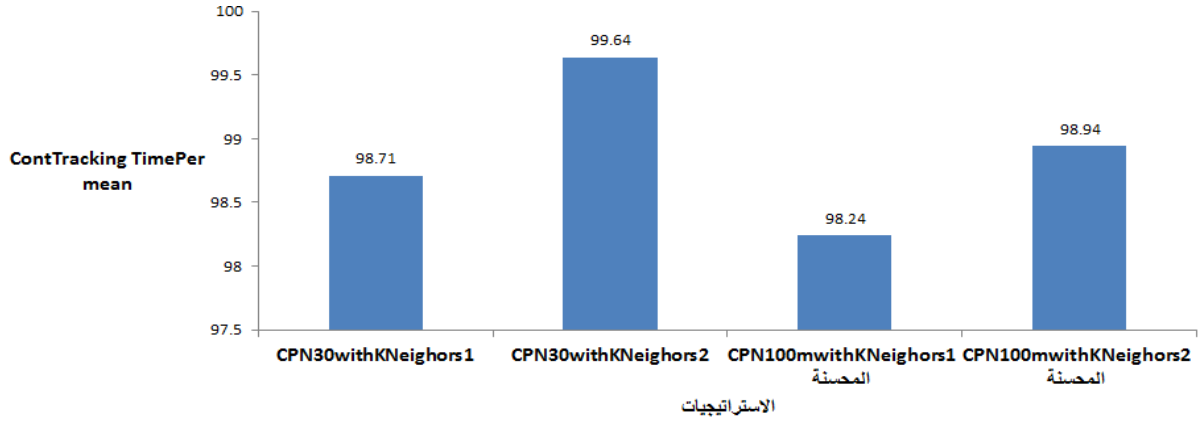
متوسط عدد مرات إرباك المهاجم يتعلق بعدد مرات تغير الاسم المستعار من قبل العربات و بالتالي سيزداد عدد مرات إرباك المهاجم بحالة SLOW40KM/H كما في الشكل (١٠). متوسط حجم مجموعة إخفاء الهوية الأعظمي يزداد بزيادة عدد العربات التي ستدخل بحالة صمت راديوي معاً و يحدث هذا الأمر عند مرور مجموعة من العربات لتقاطع معين أو انتظارها تغير اشارة المرور إلى اللون الأخضر أو بحالة الازدحام المروري و بالتالي ستنخفض سرعة تلك العربات إلى ما دون 30KM/H و بالتالي زيادة الشك لدى المهاجم(متوسط الانتروبيا الأعظمية) كما في الشكل (١١)(١٢).

2 –المقارنة بين *CPN* بحالة كان المجال الراديوي للعربة ٣٠ متر و بين *CPN* بحالة تم زيادة المجال الراديوي إلى ١٠٠متر و دراسة تأثير زيادة عدد الجوار على أداء الخوارزمية .

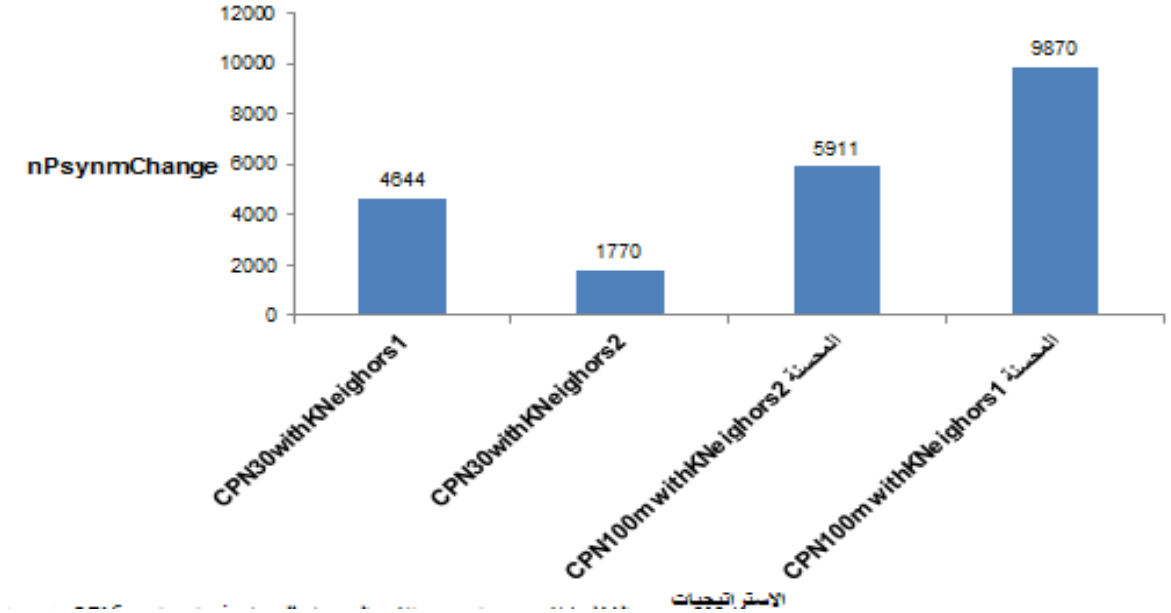
أجريت المحاكاة بحالتي : عدد جوار العربة يساوي جار واحد على الأقل K=1، بحالة زيادة عدد الجوار إلى k=2 على الأقل .



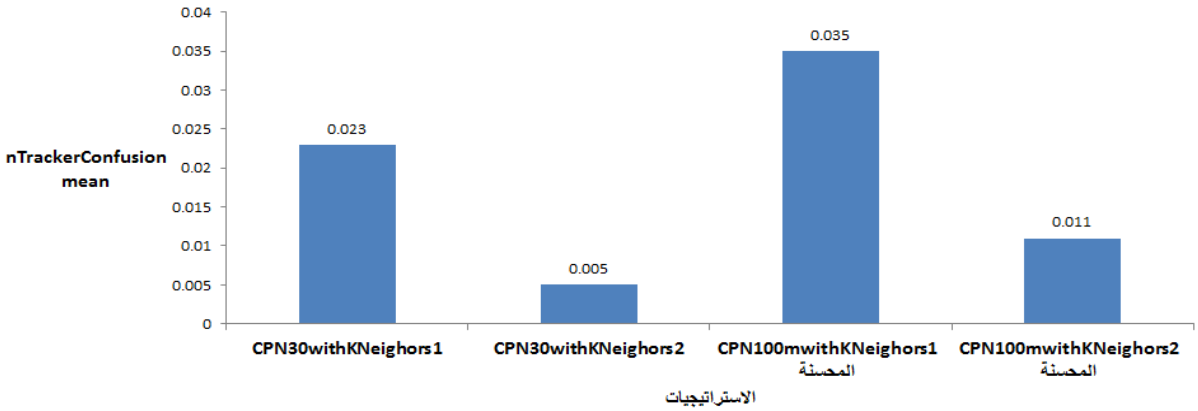
الشكل(13):يمثل متوسط عدد رسائلBeacons المستقبلة من قبل المهاجم



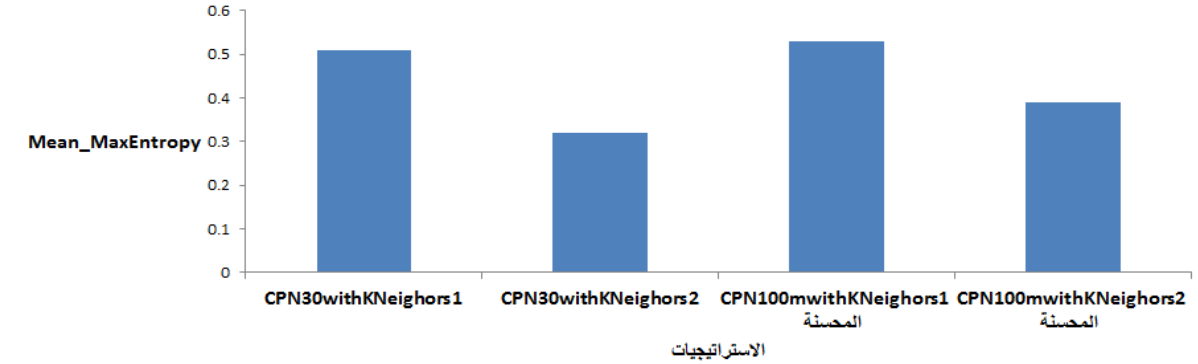
الشكل(14): يمثل متوسط النسبة المئوية لزمن التعقب المستمر



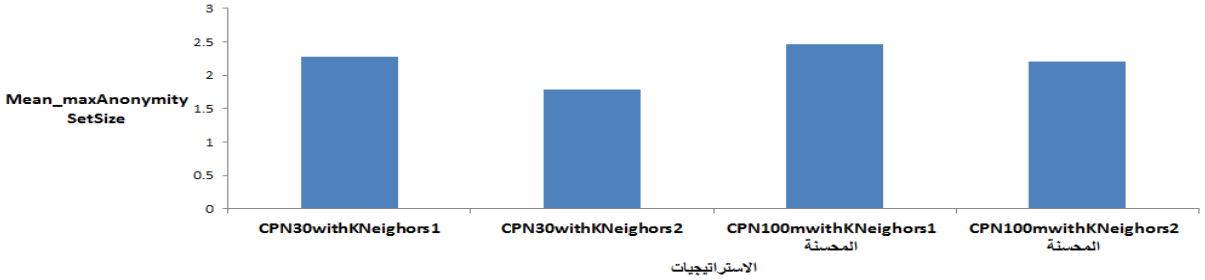
الشكل (15): يمثل عدد الأسماء المستعارة التي تم تغيرها من قبل العربات



الشكل(16):يمثل متوسط عدد مرات إرباك المهاجم



الشكل(17):يمثل متوسط الانتروبيا الأعظمية

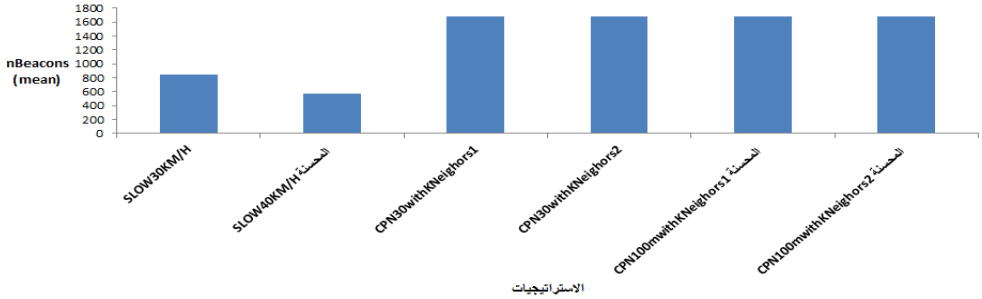


الشكل(18):يمثل متوسط حجم مجموعة إخفاء الهوية الأعظمي

يوضح الشكل (13) متوسط عدد رسائل Beacons التي تم استقبالها من قبل المهاجم ، بما إن هذه الاستراتيجية لا تعتمد على الصمت الراديوي و بالتالي لن يؤثر ذلك على سلامة الطريق . يوضح الشكل (١٤) انخفاض متوسط النسبة المئوية لزمن التعقب المستمر بزيادة المجال الراديوي للعربة و بتقليل عدد الجيران و بالتالي فإن CPN100m with K=1 يعطي أقل قيمة لمتوسط زمن التعقب المستمر . أن تجد عربة ما راغبة بتغير اسمها المستعار جار واحد على الأقل راغب بتغير اسمه المستعار معها بحالة كان مجالها راديوي ١٠٠متر هي احتمالية عالية مقارنة بحالة وجود جارين على الأقل أو بمجال راديوي ٣٠متر و بالتالي ستقوم العربة التي مجالها راديوي هو ١٠٠ متر بتغير اسمها المستعار عندما تجد جار واحد على الأقل ، عدد مرات تغير الاسم المستعار سيزداد بحالة CPN100m with K=1 مقارنة مع زيادة عدد الجيران k=2 و بنفس المجال الراديوي كما في الشكل (15). متوسط عدد مرات إرباك المهاجم يتعلق بعدد مرات تغير الاسم المستعار من قبل العربات و بالتالي فإن CPN100m with K=1 تعطي متوسط عدد مرات إرباك المهاجم أعلى مقارنة مع CPN30m كما في الشكل (16). متوسط حجم مجموعة إخفاء الهوية الأعظمي أعلى بحالة CPN100m with K=1 و بالتالي زيادة متوسط الانتروبيا الأعظمية كما في الشكلين (١٧)(١٨).

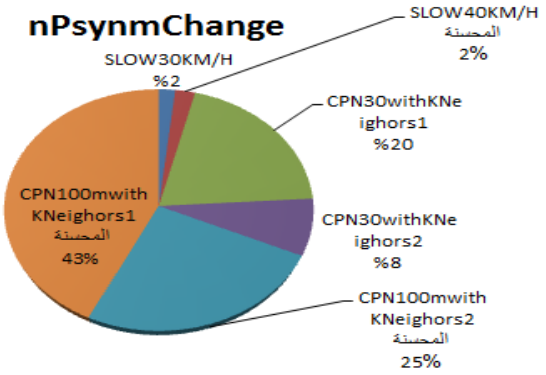
3- المقارنة بين أداء خوارزمية SLOW و CPN

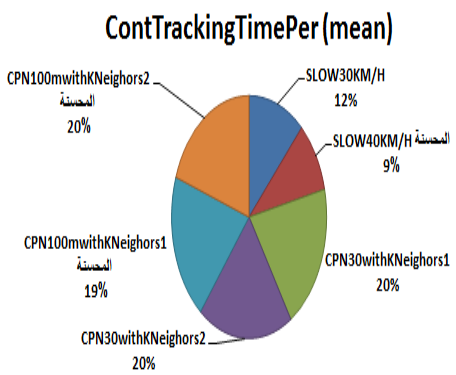
يوضح الشكل (١٩) متوسط عدد رسائل Beacons المستقبلة من قبل المهاجم ، تبقى خوارزمية CPN محافظة على قيمتها بحالة كان المجال الراديوي 100m & 30m و ذلك بسبب عدم اعتمادها على الصمت الراديوي لتغيير الاسم المستعار مقارنة مع SLOW القائمة على الصمت الراديوي.



الشكل(19):يمثل متوسط عدد رسائل beacons المستقبلة من قبل المهاجم.

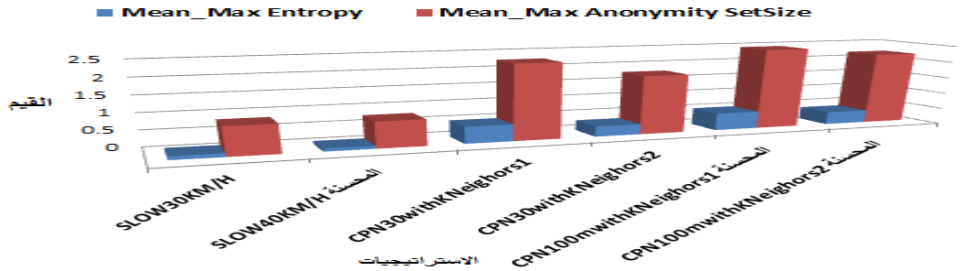
يوضح الشكل (٢٠) متوسط النسبة المئوية لزمن التعقب المستمر لكلا الخوارزميتين ، حيث حققت خوارزمية SLOW40km/h المحسنة أقل نسبة بسبب تكرار حالات دخول العربة بفترات صمت راديوي .





الشكل (٢٠):يمثل متوسط النسبة المئوية لزمن التعقب المستمر. الشكل (٢١):يمثل عدد مرات تغير الاسم المستعار من قبل العربات.

CPN تعتمد بشكل أساسي على وجود جار راغب بتغير اسمه المستعار و بالتالي احتمالية تغير العربة لاسمها المستعار سيزداد بحالة زيادة المجال الراديوي و تقليل عدد الجوار مقارنة مع SLOW المعتمدة على الصمت الراديوي لإجراء عملية التغيير كما في الشكل (٢١).يوضح الشكل (٢٢) متوسط حجم مجموعة إخفاء الهوية و متوسط الانتروبيا الأعظمية ،كلما زاد متوسط حجم مجموعة إخفاء الهوية كلما زادت متوسط الانتروبيا الأعظمية ، بحالة CPN100mwithKNeighors1المحسنة يزداد متوسط حجم مجموعة إخفاء الهوية الأعظمية مقارنة مع CPN30M و SLOW، بسبب زيادة احتمالية وجود جيران ضمن مجال راديوي ١٠٠ متر و بالتالي زيادة شك المهاجم في معرفة العربة المستهدفة.



الشكل (٢٢):يمثل متوسط حجم مجموعة إخفاء الهوية الأعظمي و متوسط الانتروبيا الأعظمية لكل من CPN&SLOW

الاستنتاجات والتوصيات

تم تقييم أداء كل من تقنية الـSlow المستخدمة لاستراتيجية الصمت الراديوي عند تغير الاسم المستعار و CPN المستخدمة لآلية trigger المحفز (عدد الجوار).

من ناحية عدد الأسماء المستعارة المستهلكة من قبل العربة : تعدّ Slow أفضل من CPN لأن تغير الاسم المستعار مرتبط بسرعة العربة ، أي أن استهلاك العربة للأسماء المستعارة سيكون أقل مقارنة مع CPN.

من ناحية الخصوصية :تعدّ CPN أفضل، كلما وجدت العربة أثناء مسيرها جار راغب بتغيير اسمه المستعار ستعسى العربة لتغير اسمها المستعار معه ، بالتالي استهلاك عدد أكبر من الأسماء المستعارة و بالتالي زيادة متوسط حجم مجموعة إخفاء الهوية الأعظمي و متوسط الانتروبيا الأعظمية .

من ناحية التعقب: كان متوسط النسبة المئوية لزمن التعقب المستمر أقل قيمة في خوارزمية SLOW40km/h بسبب احتمالية بقاء العربة تسير بسرعة أقل من 40km/h و بالتالي تكرار دخولها بفترة صمت راديوي .

بالنسبة للتوصيات المستقبلية ، إمكانية دمج كِلا التقنيتين معاً ، أي العربة T تقوم بتغير اسمها المستعار عندما تحقق شرطين هما : 1- عند انخفاض سرعتها إلى عتبة معينة .

2- وجود جار يسير بسرعة قريبة لسرعة العربة T، راغب بتغير اسمه المستعار و بالتالي يصبح Trigger عبارة عن مكونين هما (سرعة العربة ، عدد الجوار).

المراجع

[1] Sommer, C., & Dressler, F. (2014). *Vehicular networking*. Cambridge University Press.

[2] 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.

[3] Sommer, C., Eckhoff, D., & Dressler, F. (2014). IVC in cities: Signal attenuation by buildings and how parked cars can improve the situation. *IEEE Transactions on Mobile Computing*, *13*(8), 1733-1745.

[4] Doukha, Z., & Moussaoui, S. (2016). An SDMA-Based Mechanism for Accurate and Efficient Neighborhood-Discovery Link-Layer Service. *IEEE Trans. Vehicular Technology*, *65*(2), 603-613.

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

[6] Eckhoff, D., & Sommer, C. (2014). Driving for big data? Privacy concerns in vehicular networking. *IEEE Security & Privacy*, *12*(1), 77-79.s

[7] Eckhoff, D., German, R., Sommer, C., Dressler, F., & Gansen, T. (2011). SlotSwap: strong and affordable location privacy in intelligent transportation systems. *IEEE Communications Magazine*, *49*(11).

[8] Lin, X., Sun, X., Ho, P. H., & Shen, X. (2007). GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on vehicular technology*, *56*(6), 3442-3456..

[9] Wiedersheim, B., Ma, Z., Kargl, F., & Papadimitratos, P. (2010, February). Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. *In Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on (pp. 176-183). IEEE*.

[10]Schaub, F., Ma, Z., & Kargl, F. (2009, August). Privacy requirements in vehicular communication systems. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 3, pp. 139-145). IEEE.

[11] Wasef, A., & Shen, X. S. (2010). REP: Location privacy for VANETs using random encryption periods. *Mobile Networks and Applications*, *15*(1), 172-185.

[12] Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., ... & Hubaux, J. P. (2009). Secure vehicular communication systems: design and architecture. *arXiv preprint arXiv:0912.5391*.

[13] Buttyán, L., Holczer, T., Weimerskirch, A., & Whyte, W. (2009, October). Slow: A practical pseudonym changing scheme for location privacy in vanets. In *Vehicular Networking Conference (VNC), 2009 IEEE* (pp. 1-8). IEEE.

[14] Qu, F., Wu, Z., Wang, F. Y., & Cho, W. (2015). A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *16*(6), 2985-2996.

[15] Dressler, F., Kargl, F., Ott, J., Tonguz, O. K., & Wischhof, L. (2011). Research challenges in intervehicular communication: lessons of the 2010 Dagstuhl Seminar. *IEEE Communications Magazine*, *49*(5).
[16] Boualouache, A., & Moussaoui, S. (2017). Urban pseudonym changing strategy for location privacy in VANETs. *International Journal of Ad Hoc and Ubiquitous Computing*, *24*(1-2), 49-64.
[17] Papadimitratos, P., Buttyan, L., Hubaux, J. P., Kargl, F., Kung, A., & Raya, M. (2007, June). Architecture for secure and private vehicular communications. In *Telecommunications, 2007. ITST'07. 7th International Conference on ITS* (pp. 1-6). IEEE.
[18] Eckhoff, D. (2013). Privacy and surveillance: Concerns about a future transportation system. *1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2013)*, 15.
[19] Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. *Journal of computer security*, *15*(1), 39-68.
[20] Pan, Y., & Li, J. (2013). Cooperative pseudonym change scheme based on the number of neighbors in VANETs. *Journal of Network and Computer Applications*, *36*(6), 1599-1609.
[21] Wagner, I., & Eckhoff, D. (2014, December). Privacy assessment in vehicular networks using simulation. In *Proceedings of the 2014 Winter Simulation Conference* (pp. 3155-3166). IEEE Press.