IRAQI Academic Scientific Journals

Tikrit Journal of Engineering Sciences (2021) 28 (1): 31-39.

College of Engineering

ISSN: 1813-162X (Print) ; 2312-7589 (Online)

Tikrit Journal of Engineering Sciences

available online at: http://www.tj-es.com

TJES Tikrit Journal of Engineering Sciences

Shaleesh IS, Almohammedi AA, Mohammad NI, Ahmad AA, Shepelev V. Cooperation and radio silence strategy in Mix Zone to Protect Location Privacy of Vehicle in VANET. *Tikrit Journal of Engineering Sciences* 2021; **28**(1): 31- 39.

Cooperation and radio silence strategy in Mix Zone to Protect Location Privacy of Vehicle in VANET

Izdihar S. Shaleesh[1]*

Akram A. Almohammedi [2]

Naji I. Mohammad[3]

Ali A. Ahmad[4]

Vladimir Shepelev[5]

[1]Department of Communication Technology/ Faculty of Information and Communication Technology Engineering/ Tartous University/ Tartous/ Syria

[2]Automobile Transportation Department /South Ural State University/ Chelyabinsk454080/ Russia

[3]Department of Communication Technology/ Faculty of Information and Communication Technology Engineering/ Tartous University/ Tartous/ Syria

[4]Department of Communication Technology/ Faculty of Information and Communication Technology Engineering/ Tartous University/ Tartous/ Syria

[5]Automobile Transportation Department /South Ural State University/ Chelyabinsk454080/ Russia

***Keywords*:**

location privacy; VANET; radio silence; pseudonym.

ARTICLE INFO

Article history:

Received	21 Jan. 2021
Accepted	25 Feb. 2021
Available online	02 May 2021

ABSTRACT

With increase in the population, the number of registered vehicles has dramatically increased over all the world, and this leads to a high rate of traffic accidents on the roads. Therefore, in order to prevent such accidents, an Intelligent Transportation Systems (ITSs) is needed to be installed to notify drivers of obstacles in advance. Recently, the Internet of things (IoT) evolves the vehicular communications and covers this technology under the Internet of vehicles (IoV) application. IoV is a new field for the automotive industry and a significant part of the smart cities. However, protecting the privacy of vehicle's location is the most challenging subject in the vehicular communication, as because it threatens the personal life of drivers. This paper provides cooperation and radio silence strategy in mix zone (CRSMZ) to protect location privacy of vehicle in IoV. The strategy implements either cooperation or radio silence depending on the speed of the vehicle while it is in mix _zone. The simulation results show that CRSMZ is an efficient strategy to protect location information of vehicle drivers. CRSMZ outperforms the existing strategies in terms of mean of the number tracker confusion, continuous tracking period and max of the entropy.

DOI: http://doi.org/10.25130/tjes.28.1.04

* Corresponding Author: Izdihar S. Shaleesh

استراتيجية التعاون و الصمت الراديوي في منطقة المزج لحماية خصوصية موقع العربة

ازدهار شاليش / كلية هندسة تكنولوجيا المعلومات و الاتصالات / جامعة طرطوس
أكرم المحمدي / قسم النقل /جامعة ولاية جنوب الأورال / روسيا
ناجي محمد / كلية هندسة تكنولوجيا المعلومات و الاتصالات / جامعة طرطوس
علي أحمد / كلية هندسة تكنولوجيا المعلومات و الاتصالات / جامعة طرطوس
فلاديمير شيبليف / قسم النقل /جامعة ولاية جنوب الأورال / روسيا

الخلاصه

مع زيادة عدد السكان ، زاد عدد المركبات المسجلة بشكل كبير في جميع أنحاء العالم ، وهذا يؤدي إلى ارتفاع معدل حوادث المرور على الطرق. لذلك ، من أجل منع مثل هذه الحوادث ، يلزم تركيب أنظمة نقل ذكية لإعلام السائقين بالعقبات مسبقًا. في الآونة الأخيرة ، طورت إنترنت الأشياء اتصالات العربات وتغطي هذه التقنية تحت تطبيق إنترنت المركبات (IoV) . IoV هو مجال جديد لصناعة العربات وجزء مهم من المدن الذكية. إنَ حماية خصوصية موقع العربة هو الموضوع الأكثر تحديًا في اتصالات العربات، لأنه يهدد الحياة الشخصية للسائقين. توفر هذه الورقة استراتيجية التعاون والصمت اللاسلكي في منطقة المزج (CRSMZ) لحماية خصوصية موقع العربة في IoV. تنفذ الإستراتيجية إما التعاون أو الصمت اللاسلكي اعتمادًا على سرعة العربة أثناء وجودها في منطقة المزج. تظهر نتائج المحاكاة أن CRSMZ هي استراتيجية فعالة لحماية معلومات موقع سائقي المركبات. يتفوق CRSMZ على الاستراتيجيات الحالية من حيث متوسط عدد مرات إرباك المهاجم وفترة التتبع المستمر والحد الأقصى للإنتروبيا.

1. INTRODUCTION

To ensure traffic safety and mitigate accidents, attention has been paid to vehicle networks, which are one of the most important technologies intelligent transportation system [1]. Communication between vehicles is done using periodic messages called beacon messages. The beacon message includes location, velocity, direction, acceleration [2], [3]. To secure communication between the vehicles, the vehicles must be equipped with a device called on-board unit (OBU) [4], [5]. These messages are sent wirelessly, so the driver can be easily tracked by the attacker. Therefore, protecting vehicle location privacy is an important issue in an intelligent transportation system. Several privacy schemes have been proposed that discuss several methods of determining when and where a pseudonym should be changed. In [6], the authors used the Vehicular Location Privacy Zone strategy (VLPZ) to protect location privacy of vehicle based on vehicle privacy area. The authors used places where the driver time depends on the amount of service required in those places. For example, when the driver goes to the fuel station, the time required for the driver to stay at the station and Fuel filling in vehicle depends on the existing congestion in a station. Anonymity Set (AS) represents the level of privacy protection in VANET. In VLPZ, the AS is represented the vehicles existing in station, the more vehicles that reach VLPZ the higher the AS.

The authors in [7] used the Silence & Swap at Signalized Intersection strategy (S2SI), considering that the intersection was used as silent mix zones for interchange pseudonyms for only two vehicles. The entropy represents the level of specificity achieved in the strategy, relates to the number of vehicles entering the intersection and the waiting time for a traffic light to switch from red to green. The greater the waiting time, the greater the number of vehicles arriving at the intersection, and thus the greater the entropy. But this strategy needs to be controlled by the RSUs that select the vehicles for the swap operation. In [8], the authors proposed at the Velocity Based Pseudonym Changing Strategy, so that a vehicle moves at different velocities, and this depends on the driver's behavior, the nature of the road and the driving time. Consequently, there may be other vehicles that have the same velocity as this vehicle. The vehicles were divided into groups according to their velocity, where the authors found that the relationship between the rate of anonymity size and the time of stay of the vehicle in the group is an exponential relationship.

In [9], the authors took advantage of the traffic congestion within the city, which depends on the time the vehicle passes (early morning, evening, while the employees are out) to change the pseudonym to suggest a traffic-aware pseudonym changing strategy. The relationship between traffic congestion and entropy (the parameter of privacy) is an exponential relationship. In [10], the authors used Density-based Location Privacy strategy based on finding a zone called the K-density zone. For the vehicle to change its pseudonym, it is necessary K-1 From neighbors within that zone, but protection from a pseudonym's syntax attack is not guaranteed[11]. The work in this paper propose a new strategy based on choosing a method for changing the pseudonyms according to vehicle velocity and comparing the results with two existing strategies Slow and CPN. The main objectives of this study are: to increase the level of privacy required and reduce the percentage of continuous tracking time

2. System Model

In this section, the system and model of discounting are discussed.

2.1. *Vehicular Network Architecture*

Fig. 1 shows the network architecture of vehicles. The architecture consists of four basic components, which are TA (Trusted Authority), LBS (Location Based Services), vehicles and Road Side Unit (RSU). V2V is communication between vehicles, while V2I is communication between RSU and vehicles. TA and LBS connect with RSU with a secure link. TA provides certificates to vehicles through RSU with a secure link. LBS provides location information to vehicles. Each vehicle is equipped with OBU (On Board Unit) for communication with RSU and with other vehicles [7]

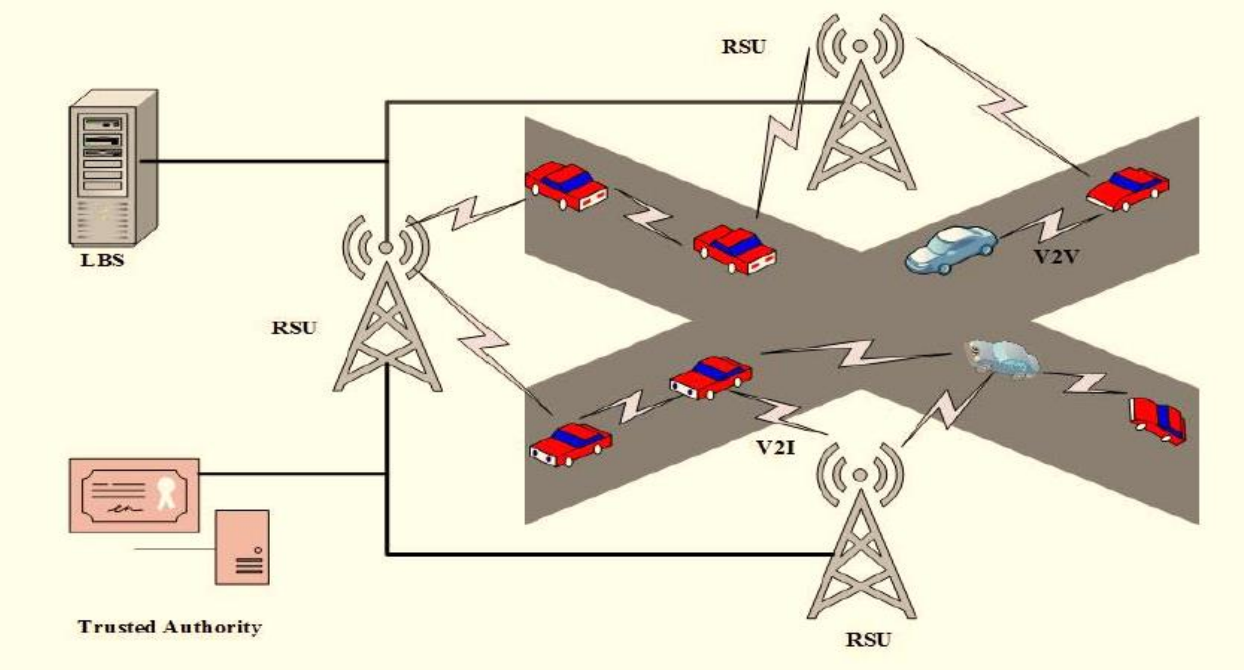

Fig. 1. Vehicle Network Architecture [7].

2.2. *Attacker model*

The effectiveness of the proposed system against the global passive attacker has been studied, whereby the attacker can track the vehicle located within the area of interest, knowing that he is aware of the network model and the technology used to protect the location's privacy.

2.3. *Cooperation and radio silence strategy in Mix Zone*

This paper tackles the problem of protecting the location privacy of drivers in VANETs. The pseudonym changing approach is suggested as a solution to this problem, while the development of an effective pseudonym changing strategy is still one of the open issues. Figs. 2 describes the system that each vehicle and RSU start registration at trusted authority (TA). Each vehicle obtains the public and private keys from the TA. The public key is used as a pseudonym and the private key is used for the signing beacon message. The receiving vehicle verifies the authenticity of a beacon message the public key of the vehicle. The proposed strategy is based on the existence of mix zones (a traffic intersection or spot social or highway). When the vehicle reaches a zone, it is grouped depending on its speed. If its speed is within the low speed limits, it enters the radio silence, after that it performs the process of changing the pseudonym. The vehicle uses the mode of cooperation with its neighbors to carry out the process of changing the pseudonym with them in order to confuse the attacker knowing the target vehicle if its speed is within 40 and 60 km / h. If the vehicle finds the number of its neighbors greater or equal to the threshold and the neighbors' ready flag received is 1, then it places its ready flag = 1 and performs the process of changing the pseudonym with them. Then it returns its ready flag to zero. In the event that the vehicle is traveling at a speed greater than 60 km / h, then you make the flag of readiness equal to zero and carry out the process of changing the pseudonym.

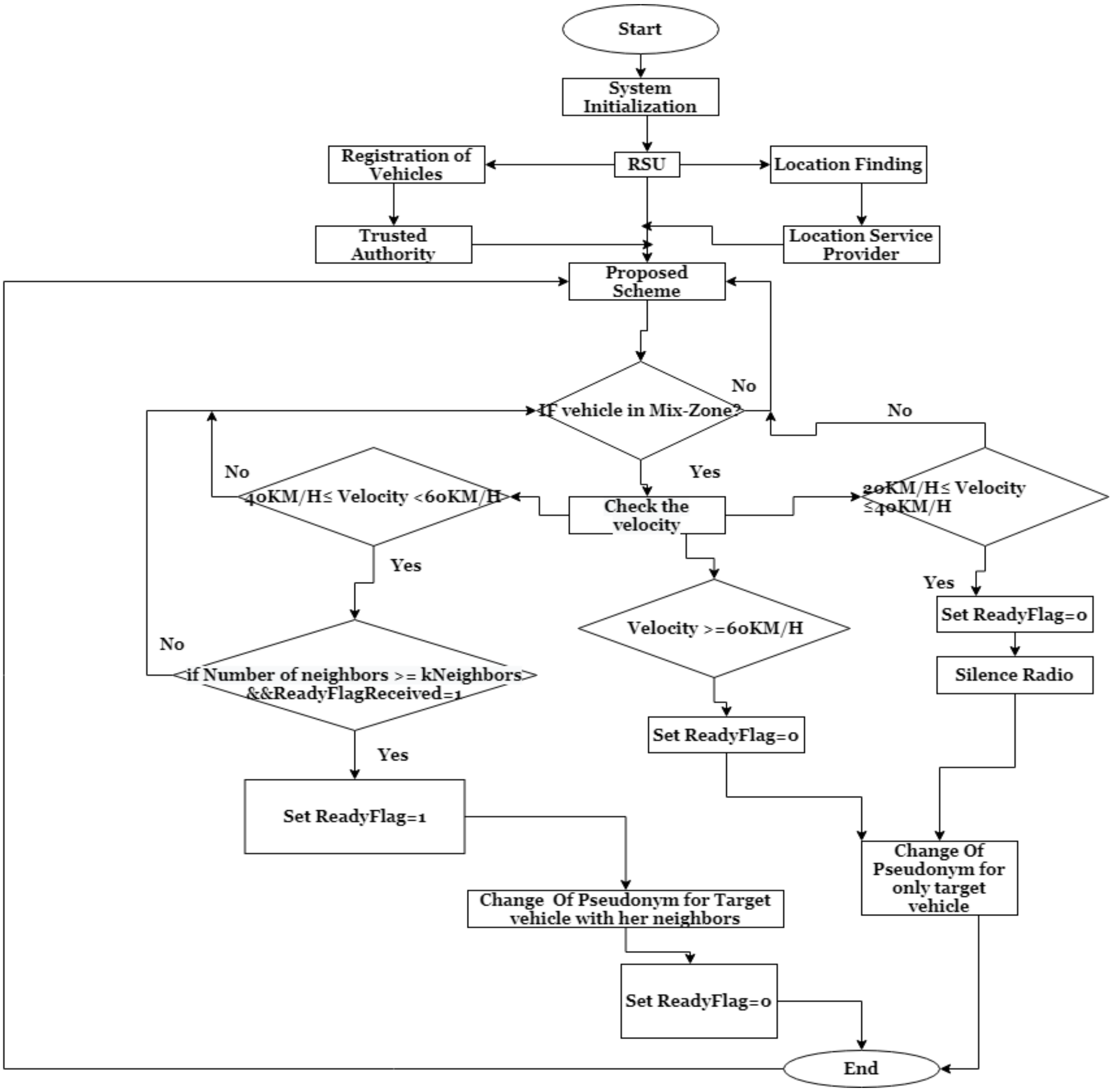

Fig. 2. Cooperation and radio silence strategy in Mix Zone

3. RESULTS AND DESCUSSION

In this section, the proposed scheme is analyzed in terms of robustness against passive adversary attack and compare it with existing techniques SLOW [12] and CPN [13]using the tracking and the privacy metrics. The simulation is carried out using Sumo, Omnet and Veins [14] - [18]. Table 1 shows simulation parameters used in the experiments.

Table 1
Simulation Parameters

Strategy	Parameter	Default Value
CPN	Radius	100m
	Neighbors Threshold	2
SLOW	Velocity Threshold	40km/h
	Silent Threshold	5 s
Proposed Technique (CRSMZ)	Radius	100m
	Neighbors Threshold	2
	Silent Threshold	5 s

3.1. Results of the number of times the pseudonym changed

Figs. 3 describes the number of times vehicles that have changed their pseudonyms.

In CRSMZ, the vehicle can permanently change its pseudonym if it is within the Mix Zone. Thus, the average number of times the pseudonym is changed high compared to a condition CPN that it needs to be changed at least two neighbors, while SLOW is requiring that its speed be reduced to less than 40km/h.

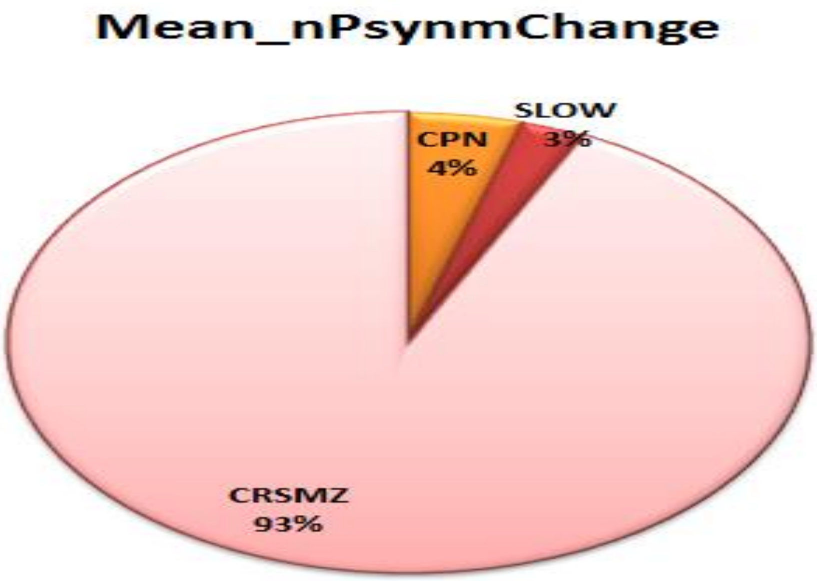

Fig. 3. Mean_nPsynmChange

3.2. Continuous Tracking Percentage Result

Figs. 4 shows the maximum period of time during which the attacker is able to trace the beacon messages to one vehicle without accidentally assigning one of its messages to another vehicle. In CRSMZ, the mean_contTrackingTimePer is low , because of the constant change of pseudonym

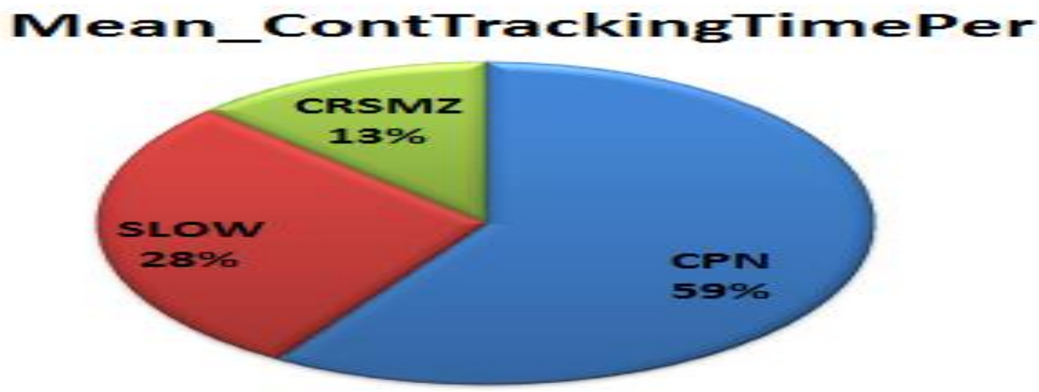

Fig. 4. Mean Continuous Tracking Percentag.

3.3. Average number of confusions

When an attacker makes a mistake in assigning a beacon message to a vehicle and thus becomes confusing in following the target vehicle. Fig. 5 shows higher mean nTracker confusion for CRSMZ compared to the existing strategies, this is because the constant change in the pseudonym for CRSMZ causes high confusion for the attacker.

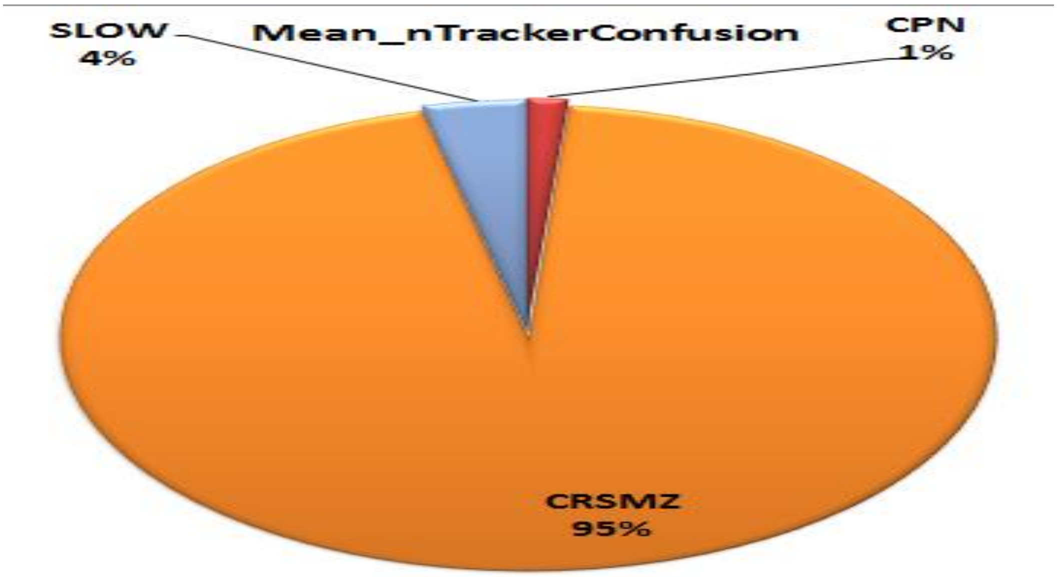

Fig. 5. Mean nTracker Confusion

3.4. Mean Max Anonymity set size

Mean Max Anonymity set size represents the group of the existing vehicles, including the target itself. The CRSMZ strategy represents the group of vehicles within the mixing area. The CPN strategy represents the cooperating vehicles to change the pseudonym. SLOW strategy represents a vehicle whose velocity is less than 40km/h. Fig. 6 displays that mean max anonymity set size in the CRSMZ is higher than CPN and SLOW.

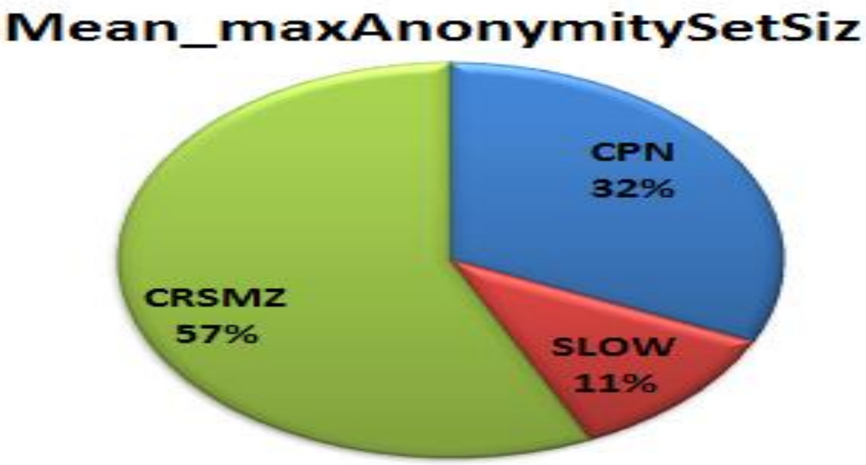

Fig. 6. Mean_MaxAnonymitySetSize.

3.5. Mean Max Entropy

The entropy of the anonymity set allows expressing the adversary's knowledge about each vehicle of the anonymity set. When mean max anonymity set size is high, the mean max entropy is also high, so the mean max entropy is high in CRSMZ as shown in Fig. 7.

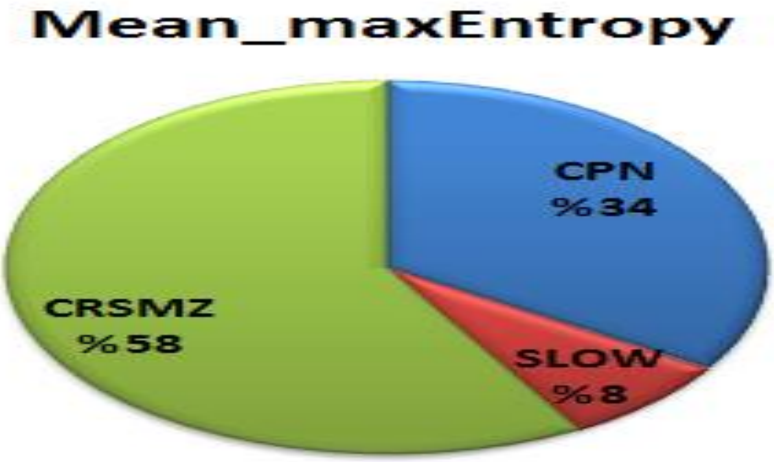

Fig. 7. Mean_MaxEntropy.

4. CONCLUSIONS

CRSMZ is a new technology proposed to protect the privacy of the vehicle's location in VANET. When the vehicle is in the mix zone, it changes its pseudonym according to its speed limit. In this case, if a vehicle is: i) at low speeds, it enters a state of radio silence, ii) at medium speeds, it requires the cooperation of its neighbors to make the change process together, iii) in high speeds, it performs the process of changing the pseudonym. The experimental results show that the proposed CRSMZ strategy shows performance improvement in terms of tracking metric (Mean Continuous Tracking Percentag13%, Mean n Tracker Confusion 95%) and privacy metric (Mean Max Anonymity Set Size 57%,Mean Max Entropy58%) compared to the existing CPN and SLOW strategies. More experiments on CRSMZ to evaluate its performance in various scenarios are recommended for future work.

REFERENCES

[1] Almohammedi, A. A., Noordin, N. K., & Saeed, S. (2016). Evaluating the Impact of Transmission Range on the Performance of VANET. International Journal of Electrical and Computer Engineering, 6(2), 800.

[2] Gasmi, R., & Aliouat, M. (2019, June). Vehicular Ad Hoc NETworks versus Internet of Vehicles-A Comparative View. In 2019 International Conference on Networking and Advanced Systems (ICNAS) (pp. 1-6). IEEE.

[3] Abdullah Q, Abdullah N, Balfaqih M, Shah NS, Anuar S, Almohammedi AA, Salh A, Farah N, Shepelev V. Maximising system throughput in wireless powered sub-6 GHz and millimetre-wave 5G heterogeneous networks. Telkomnika. 2020;18(3):1185-94.

[4] Almohammedi, A. A., & Shepelev, V. (2021). Saturation Throughput Analysis of Steganography in the IEEE 802.11 p Protocol in the Presence of Non-Ideal Transmission Channel. IEEE Access, 9, 14459-14469.

[5] Ahmed MS, Shah NS, Ghawbar F, Jawhar YA, Almohammedi AA. Filtered-OFDM with channel coding based on T-distribution noise for underwater acoustic communication. Journal of Ambient Intelligence and Humanized Computing. 2020: 1-14.

[6] Boualouache, A., Senouci, S. M., & Moussaoui, S. (2016). Vlpz: The vehicular location privacy zone. Procedia Computer Science, 83, 369-376.

[7] Boualouache, A., & Moussaoui, S. (2014, June). S2si: A practical pseudonym changing strategy for location privacy in vanets. In 2014 International Conference on Advanced Networking Distributed Systems and Applications (pp. 70-75). IEEE

[8] Ullah, I., Wahid, A., Shah, M. A., & Waheed, A. (2017, April). VBPC: Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET. In 2017 International Conference on Communication Technologies (ComTech) (pp. 132-137). IEEE.

[9] Boualouache, A., & Moussaoui, S. (2017). TAPCS: Traffic-aware pseudonym changing strategy for VANETs. Peer-to-Peer Networking and Applications, 10(4), 1008-1020.

[10] Song, J. H., Wong, V. W., & Leung, V. C. (2010). Wireless location privacy protection in vehicular ad-hoc networks. Mobile Networks and Applications, 15(1), 160-171.

[11] 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.

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

[13] 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.

[14] Emara, K., Woerndl, W., & Schlichter, J. (2013, June). Vehicle tracking using vehicular.

[15] Izdihar, S., Naji, M., Ali, A(2019, September). The Effect of Suggested Mix-Zones on the Privacy Protection of Vehicles' Location in VANET Networks. (41).Al Baath Magazine.

[16] 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

[17] Izdihar Sh (2020). The Privacy protection of the vehicle location in vehicular ad hoc networks. Journal of Bakht Al-Ridha, (31).

[18] Hassan, A .,Ali, A., Nawaf M (2007). Replacement of VRRP Protocol by Router Clustering. Tishreen University Journal.(29).