A Flickering Context-based Mix Strategy for Privacy Protection in VANETs

Zhixiang Zhang, Tianyi Feng, Biplab Sikdar and Wai-Choong Wong
Department of Electrical and Computer Engineering,
National University of Singapore,
Singapore 119077
Email: e0320869@u.nus.edu, fengtianyi@u.nus.edu, bsikdar@nus.edu.sg, wong_lawrence@nus.edu.sg

***Abstract*—Vehicular Ad-Hoc Networks (VANETs) are a significant part of Intelligent Transportation Systems (ITS), and they are used to enhance the road safety and improve the traffic efficiency through the communication between vehicles and roadside units. However, some malicious adversaries can use the periodically broadcast beacons in VANETs to track vehicles. To mitigate this threat and protect privacy, existing research primarily suggests the use of pseudonyms as variable identities for each vehicle, and has explored different pseudonym mix strategies. These mix strategies often introduce latent traffic accident risks by requiring the vehicles to change their driving behavior or stop broadcasting. In this paper, we present a flickering context-based mix strategy, which can reduce such hidden dangers and provide higher privacy level than traditional context-based strategy. Besides, we employ a passive global adversary to evaluate the proposed strategy and conduct simulations in both virtual maps and real city maps to measure the protection level of the proposed privacy scheme. Finally, the influences of different parameters in our new method are explored.**

***Index Terms*—privacy, pseudonym, VANETs**

I. Introduction

With the rapid development of communication networks, their new features of low latency and large bandwidth are enabling new applications. As more and more intelligent devices participate in the Internet of Things (IoT) [1], people's lives have become more convenient. The concept of Smart City [2] has been proposed to allow city officials to manage and monitor directly with both community and city infrastructure. Vehicular Ad-Hoc Networks (VANETs) [3], which consists of trusted authority (TA), on board unit (OBU), and roadside unit (RSU), aim to improve road safety and efficiency by sharing the state of vehicles. To do so, IEEE, ETSI, and SAE [4] suggest vehicles to broadcast safety messages periodically. These messages contain the position, speed, heading and identity of each vehicle. However, these messages also expose the vehicle's trajectory and are thus a privacy risk.

Lim, et al. [5] classified three types of privacy to be protected in VANETs: the vehicle's identity, location, and the data exchanged. Since the data can be protected by encryption mechanisms, the primary issue is to protect the identity and location. To cope with it, researchers [6]–[8] have suggested the use of pre-generated pseudonyms by vehicles when they broadcast their safety messages and deploy a pseudonym changing strategy to protect vehicles from being tracked, where a pseudonym is defined as a fictive identifier [9], and only the trusted authority knows the mapping between the real identifier of a vehicle and its pseudonyms. The related previous pseudonym mix strategies may be divided into three categories:

(1) *Time-based mix strategy.* In this strategy, vehicles change their pseudonyms by following a periodic schedule. Vehicles first stop broadcasting their safety messages at time t, and they use a new pseudonym after Δt. However, this method is easy to attack, Wiedersheim et al. [10] claimed that the tracking accuracy for a global adversary almost reaches 100% in some cases. Huang et al. [11] proposed the concept of random silent period, with the intuition that if Δt was chosen randomly, it would be harder for the adversary to track individual vehicles. Further Sampigethaya et al. [12] adopted it into a group protocol.

(2) *Zone-based mix strategy* [13]. In this strategy, vehicles change their pseudonyms when they enter some predefined road sections or social spots [14]. The RSU is the coordinator [15] of such a process. These areas are also named mix-zones. However, under the assumption that the attacker has information of vehicles before they enter the mix zone, Buttyan et al. [16] claimed that the success rate of tracking a vehicle can reach up to 70%. Also, they suggested that a vehicle could improve its privacy level by changing driving behavior [17]. Boualouache, et al. [18], [19] proposed to set silent mix-zones at some public areas such as signalized intersections. In addition, some research works have explored the optimal deployment [20]–[22] of mix-zones.

(3) *Context-based mix strategy.* The two methods introduced above have various drawbacks. Time-based methods waste pseudonyms if only one vehicle changes its pseudonym while its neighbors stay unchanged. Zone-based methods have hidden danger when silent mix-zones are set in intersections, and the drivers must be highly cooperative when required to speed up or slow down. Thus, context-based methods which improve the shortcomings of previous methods have been proposed. Gerlach and Guttler. [23] suggested a method where a vehicle changes its pseudonym when it detects k neighboring vehicles within a threshold range and moving in a similar direction. Liao et al. [24] proposed to add the speed and the road segment information into the context. Recent surveys [25], [26] recommended this method because it can find high-quality opportunities for pseudonym changing.

The structure of the remaining content is organized as follows: In Section II, we discuss the traditional context-based mix strategy and the metrics used to evaluate its performance. In Section III, to overcome the shortcomings of existing methods, we propose a new context-based strategy. The details of the adversary model for privacy evaluation is presented in Section IV. Finally, we present our simulation results in Section V, and conclude the paper in Section VI.

II. Traditional Context-based Mix Strategy and Metrics

Context-based methods are user-centric, and vehicles independently determine when and where to change pseudonyms. Since they do not share any pseudonym changing records with other parts in the VANETs, even if the communications are intercepted, the adversary cannot find any direct record of a pseudonym change. To do so, traditional context-based methods [24] assume that vehicles monitor the traffic by receiving safety messages from other vehicles. Once they find there are k neighbors with similar running status, they can then change their pseudonyms together, and there is a minimum stable time for a new pseudonym.

As shown in Fig. 1, context-based mixing utilizes both the concept of mix-zone and silent period Δt together. A vehicle creates an invisible mix-zone around itself and finds k neighbors in it with similar states at time t. Then, all vehicles in this zone stop broadcasting for a silent period Δt. After that, the vehicles change their pseudonyms. Since the traffic environment and the vehicle states at the end are different from those at the start of the process, the adversary would find it difficult to track the vehicles. To evaluate the performance of pseudonym changing approach, we choose the following four objective metrics.

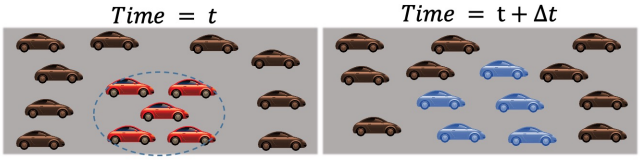

Fig. 1: Context-based mix strategy.

1) Entropy: Entropy refers to the uncertainty in information, and a system with higher entropy usually has more uncertainty. In a pseudonym changing process, let i be the old pseudonym of a vehicle, $i \in V_{in}$, where V_{in} is the set of pseudonyms of a group of vehicles that are ready to change their pseudonyms. The new pseudonym of the vehicle is denoted by j, $j \in V_{out}$, where V_{out} is the new set of pseudonyms for the vehicles with pseudonyms in V_{in}. P_{ij} is the probability that an old pseudonym i and a new pseudonym j belong to the same vehicle. The traditional method usually has $|V_{in}| = |V_{out}|$, and assume $w = |V_{out}|$, $P_{ij} = 1/w$. We use H_i to represent the entropy for vehicle i, and H_{old} to denote the total entropy of the entire process for the traditional method. Then

$$H_i = -\sum_j P_{ij} \log P_{ij} = \log 1/w, \tag{1}$$

$$H_{old} = \sum H_i = -w \log 1/w, \tag{2}$$

2) Untraceable quantity: Entropy is an abstract concept, and does not reflect the success of a real adversary. Thus we also develop a new metric called "untraceable quantity" to directly quantify how many vehicles cannot be tracked in a scenario. We discuss this model in detail in Section IV.

3) The number of pseudonyms used: Pseudonym is a resource for vehicles. If they change pseudonyms with high frequency, the pseudonym pool would run out in a short time. Besides, the authentication process is also required after each new pseudonym is applied. Thus we take the number of pseudonyms used as a measure of the cost.

4) The number of silent slots: The silent period is used to reduce the linkability between a new pseudonym and an old pseudonym. However, it results in traffic information loss, especially in intersections where a number of vehicles may have stopped, which reduces the safety of the transportation system [27]. Here, we use the number of silent slots as an indicator of the road safety.

III. Proposed Context-based Mix Strategy.

Traditional context-based methods as shown in Fig. 1, have two potential problems to be improved. First, vehicles usually start changing pseudonyms when they find a sufficient number of neighbors. If they all go into silent period, there is a potential collision risk and other dangers due to the absence of any messages. Second, the traffic environment at time $t + \Delta t$, is different from that in time t, as these vehicles could meet new neighbors during the silent period. These new vehicles can be added to our new process to increase the size of the anonymity set.

Based on the discussion above, we propose a flickering context-based mix strategy. Its flowchart can be seen in Figs. 3 and 4, and the process is displayed in Fig. 2.

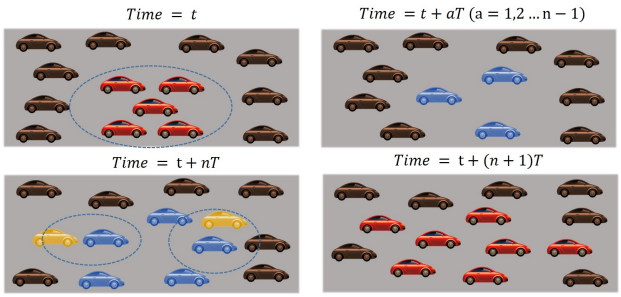

Fig. 2: The proposed strategy.

Step-1: In the beginning, at time t, k vehicles with free-state (we define vehicles those are not in the pseudonym changing process to have free-state) are ready to change pseudonyms.
Step-2: At time $t + aT$ $(a = 1, 2, \ldots n-1)$, each vehicle independently determines whether to broadcast with probability p, and if they broadcast, they will use the new pseudonym. We call this the flickering process.
Step-3: At time $t + nT$, all vehicles go into the hiding tail process. They set HT (hiding tail) as 1, and send it to new neighbors (yellow cars) who have free-state.

Step-4: All vehicles and their new neighbors who receive HT=1, change their pseudonyms at time $t + (n + 1)T$.

Let the total number of silent slots in the traditional method be denoted by N_s. In the proposed method, since vehicles broadcast with probability of p, so the number of silent slots becomes pN_s $(0 \leq p \leq 1)$, which is less than N_s. As a result, the proposed method has less impact on traffic information sharing. In the evaluation of entropy, assuming V_h new neighbors added in *steps 3 and 4* (hiding tail process), we use the notation $u = |V_h|$, and let N_h be the number of neighbors that have changed pseudonyms for vehicle $h \in V_h$, $(N_h \geq 2)$. Then the entropy for the new method is:

$$H_h = -\log 1/N_h, \tag{3}$$

$$H_{new} = \sum_i H_i + \sum_h H_h = -w \log \frac{1}{w+u} - \sum_h \log \frac{1}{N_h}, \tag{4}$$

where H_h is the entropy for vehicle h and H_{new} is the total entropy for the new strategy. Comparing the right hand terms of (2) and (4), we can see $-w \log \frac{1}{x+u} \geq -w \log \frac{1}{w}$, since $u \geq 0$. Thus $H_{new} \geq H_{old}$, and we get higher privacy level.

IV. Adversary Model

Safety messages which include the position, speed, and the heading of each vehicle, are required to be broadcasted to improve the traffic efficiency and safety. However, a passive adversary can eavesdrop these messages, and get the complete movement pattern of each vehicle. After a pseudonym changing strategy is deployed, from the adversary's view, the complete trajectory is interrupted and it faces a typical multiple target tracking (MTT) problem [28]. Researchers in [7], [29] have proposed solutions and algorithms for this problem, and one of the most commonly used model is Kalman filter. The adversary model is given as:

$$x_t = Ax_{t-1} + b, \tag{5}$$

$$z_t = Hx_t, \tag{6}$$

where A is the transition matrix, b is the Gaussian-distributed noise, $x_t = [p_t, v_t, a_t]^{Tra}$, p_t, v_t, a_t are the position, velocity and acceleration for vehicle at time t, with

$$A = \begin{pmatrix} 1 & T & T^2/2 \\ 0 & 1 & T \\ 0 & 0 & 1 \end{pmatrix}, H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \tag{7}$$

$$b = \left[\frac{T^2}{2}, T, 1\right]^{Tra} \sigma_{ap}^2, \tag{8}$$

Assuming that the interval length of the time slot is T , the covariance matrices Q and R are defined as:

$$Q = \begin{pmatrix} \frac{T^4}{4} & \frac{T^3}{2} & \frac{T^2}{2} \\ \frac{T^3}{2} & T^2 & T \\ \frac{T^2}{2} & T & 1 \end{pmatrix} \sigma_{ap}^4, R = \begin{pmatrix} \sigma_p^2 & 0 & 0 \\ 0 & \sigma_v^2 & 0 \\ 0 & 0 & \sigma_{ap}^2 \end{pmatrix} \tag{9}$$

where σ_{ap}^2, σ_v^2, σ_p^2 are the acceleration, velocity and position variances, respectively. The update is given by:

$$\hat{x}_t^- = A\hat{x}_{t-1}^-, \tag{10}$$

$$P_t^- = AP_{t-1}A^{Tra} + Q, \tag{11}$$

$$S = HP_t^- H^{Tra} + R, \tag{12}$$

$$K = P_t^- H^{Tra} S^{-1}, \tag{13}$$

$$\tilde{z}_t = z_t - H\hat{x}_t^-, \tag{14}$$

$$\hat{x}_t = \hat{x}_t^- + K\tilde{z}_t, \tag{15}$$

$$P_t = (I - KH)P_t^-, \tag{16}$$

where I is the identity matrix, and the details about the derivation can be found in [30]. With Kalman filtering, we can predict the state of vehicle in future, and the error for the prediction d_{ij}^2 in assigning j to i is calculated as:

$$d_{ij}^2 = \tilde{z}^{Tra} S^{-1} \tilde{z}, \tag{17}$$

As the new pseudonym j only belongs to one vehicle in V_{in}, data association techniques are used to avoid an incorrect or sub-optimal solution for the assignment. In this paper we apply the nearest neighbor probabilistic data association (NNPDA) technique [31], as it allows real-time calculations even when there are a large number of vehicles [32]:

$$G_{ij} = \frac{e^{-d_{ij}^2/2}}{(2\pi)^{N_m/2}\sqrt{|S_i|}}, \tag{18}$$

$$P_{ij} = \frac{G_{ij}}{T_i + M_j - G_{ij}}, \tag{19}$$

where the Gaussian likelihood function G_{ij} is associated with the assignment of a new pseudonym $j \in V_{out}$ to the old one $i \in V_{in}$. T_i is the sum of likelihood functions G_{ij} of vehicle i, M_j is the sum of G_{ij} for new pseudonym j, and $|S_i|$ indicates the determinant of the residual covariance matrix which is obtained from (12). N_m refers to the dimension of the observed vector z_t. P_{ij} is the final probability of mapping a new pseudonym j to old pseudonym i. If the $\arg\max_j P_{ij}$ is not the true pseudonym i, then i is regarded as untraceable. We count all the untraceable vehicles and denote it as the metric "untraceable quantity".

The adversary model above is applied to a traditional context-based method, which is under the assumption that all vehicles go into silent period together and once the adversary knows the length of silent period, then he or she can get the tracking results (17) by using a Kalman multi-step predictor [33], [34].

As vehicles broadcast safety messages with a probability of p at each internal time slot in the proposed method, the adversary model needs to be refined. As shown in Fig. 5, assuming that the process length is $n = 1$, there are m $(m = 3\ in\ Fig.\ 5)$ vehicles broadcasting safety messages in the middle time slot M. To let the adversary make full use of the traffic information, the new expression for G_{ij} is:

$$G_{ij} = \hat{G}_{ij} + \sum_{a=1}^{m} G_{iM_a} G_{M_a j}, \tag{20}$$

Now, G_{ij} is the combination of direct prediction and step-by-step hypothesis, where $\hat{G}_{ij}$ is obtained from (18) by setting the filter step size as 2, G_{iM_a} and $G_{M_a j}$ are calculated by

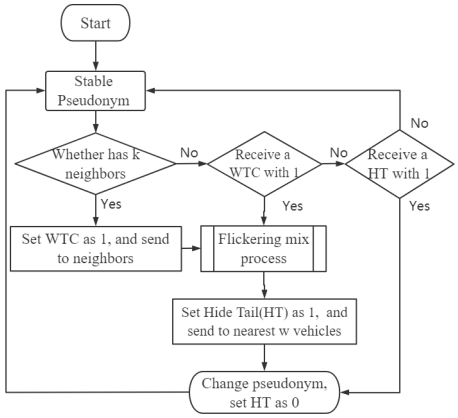

Fig. 3: Flowchart of new method.

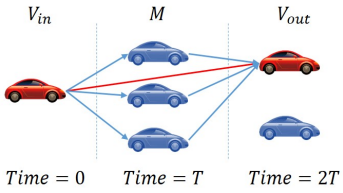

Fig. 5: Adversary model for proposed method.

setting the step size as 1. The remaining part of the adversary model is consistent with that for the traditional method. We apply this model to evaluate the untraceable quantity in the next simulation section.

V. SIMULATIONS

To make a direct comparison and evaluate the new strategy, we conduct simulations using "Simulation of Urban MObility" (SUMO) [35], [36], which is an open source, highly portable, microscopic traffic simulation package designed to handle large networks. It can not only customize the map we want, but also import the scenario from realistic city maps.

Virtual map: We created a Manhattan mobility model [37] in SUMO, as shown in Fig. 6, with a topography of 1km $\times$ 1km with four lanes in each edge. The arrival of vehicles are assumed to follow a Poisson process. A probabilistic approach is employed in the selection of vehicle's route. At each intersection, the vehicle goes straight with probability 0.5 and takes a left or right turn with probability 0.25 each.

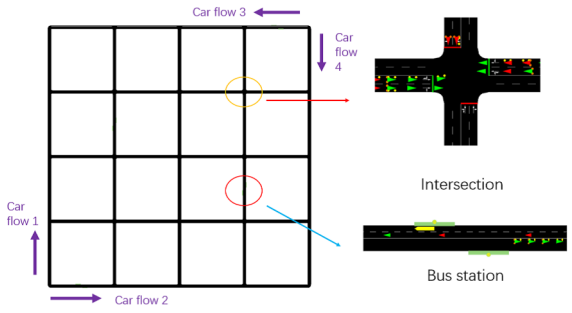

Fig. 6: Manhattan mobility model.

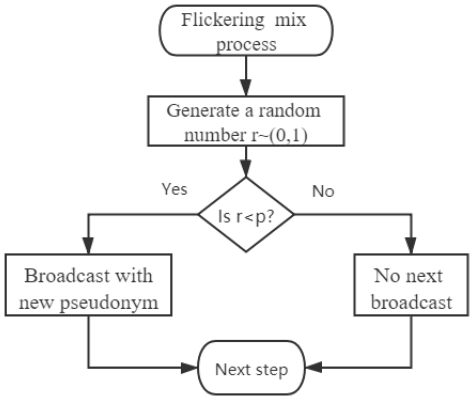

Fig. 4: Flowchart of mix process.

We also add buses to ensure that the traffic is similar to real scenarios. Buses have fixed routes and take a 30 s break at a predefined bus station which is located in the south-east sector of the second ring road. The parameters of vehicles are set as:

Type	Acceleration	Deceleration	Length	MaxSpeed
Car	$3m/s^2$	$7m/s^2$	$3m$	$17m/s$
Bus	$2.5m/s^2$	$4.5m/s^2$	$10m$	$14m/s$

TABLE I: Vehicle settings.

Real map: CBD (central business district) in southern Singapore: Singapore is large city with diverse traffic networks. As shown in Fig. 7, we select a part of CBD in southern Singapore, which is 7 km in length and 3.5 km in width. Cars and buses are added from each segment of the road, and we define the number of vehicles generated per hour and lane-kilometer, to be 14 and 1, respectively. All vehicles randomly choose their routes.

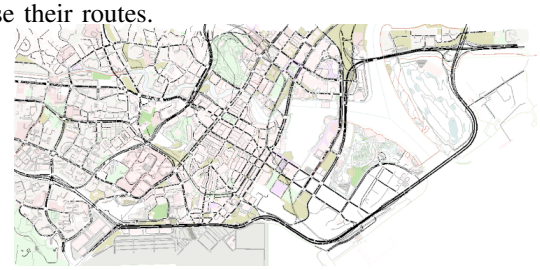

Fig. 7: CBD in southern Singapore.

The following results show the influence of different parameters on system performance. The parameters are the threshold: k, the probability of broadcasting: p, the length of process: n, and the noise in position data: e. To optimize the performance of different methods, we remove the stable time for a pseudonym.

A. Threshold: k

Vehicles start changing their pseudonyms when they find at least k neighbors. As shown in Fig. 8, the dashed lines indicate the simulation results in the virtual map, solid lines are for the real map, lines with plus sign are for the proposed context-based method, and lines with star sign are for the traditional method. We run the simulation for 100 s. When k is

small, vehicles change their pseudonyms more frequently. As k becomes larger, fewer pseudonyms and silent slots are needed, and the level of privacy protection declines. We can see our proposed method always has higher entropy and untraceable quantity.

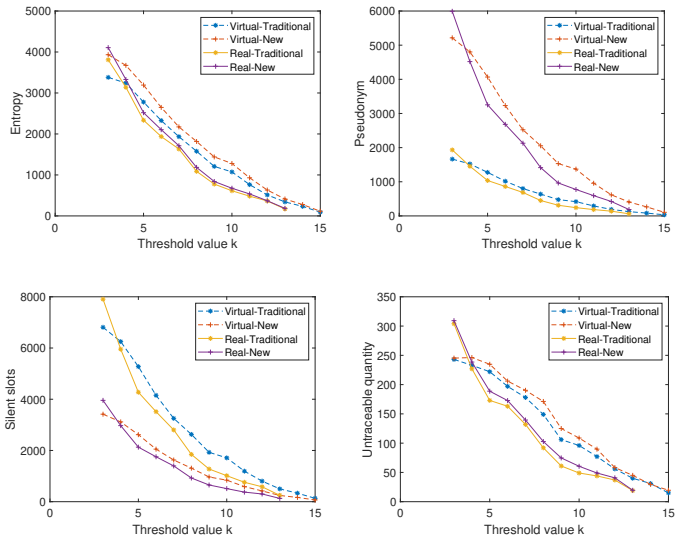

Fig. 8: Influence of k (p=0.5, n=4, e=3).

B. The probability of broadcasting: p

In the traditional pseudonym changing process, all vehicles are in silent period, and thus, $p = 0$. In the proposed strategy, p is variable. As shown in Fig. 9, p does not have obvious influence on entropy, and when p increases, there are fewer silent slots, which means the system is safer. Even though the adversary can use more messages for tracking and the untraceable quantity has a slightly decrease, the privacy protection level is still higher than that in the traditional method.

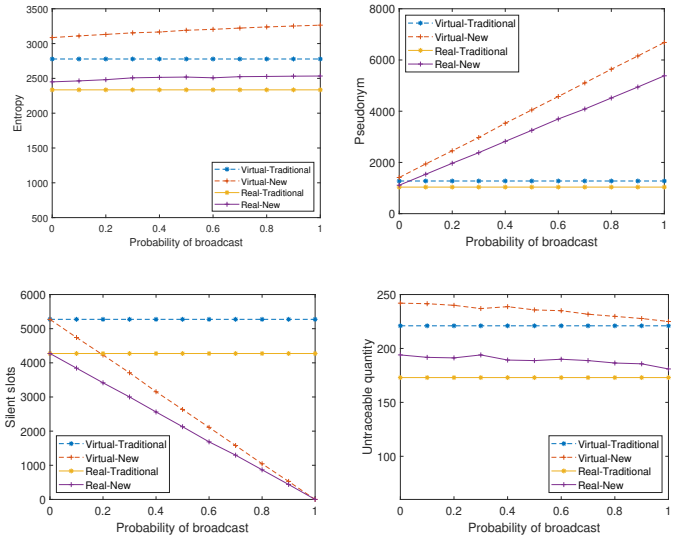

Fig. 9: Influence of p (k=5, n=4, e=3).

C. The length of process: n

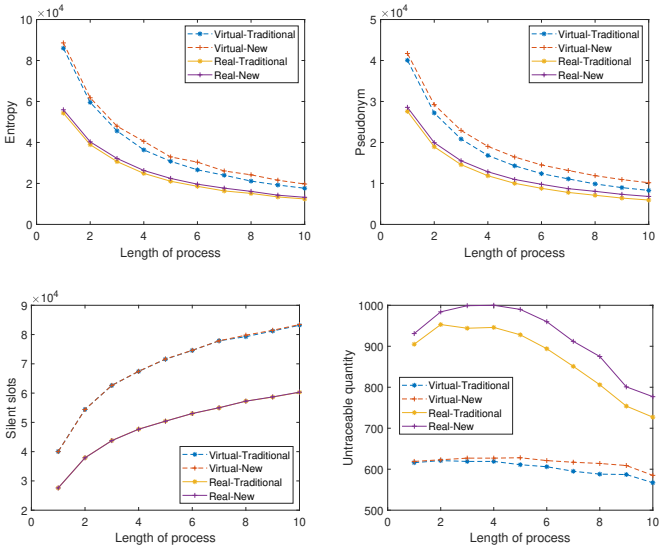

Fig. 10: Influence of n (k=5, p=0, e=3).

n is the number of time slots in the pseudonym changing process. As n increases, it is reasonable to see the increase in silent slots and the decrease in entropy and pseudonyms, because the number of repetitions for pseudonym changing process is reduced. In Fig. 10, we observe that the untraceable quantity first increases and then decreases. A longer interval brings less correlation between pseudonyms, and as a result, the untraceable quantity increases. However, as n increases, since we fix our simulation duration, the number of repetitions takes the main influence. The turning point for the traditional method is $n = 2$, and for the proposed method it is $n = 4$ or $n = 5$. This implies that the proposed method has higher resistance to the decrease of repeat times, and the quality of each pseudonym change is higher.

D. The noise in position data: e

In real life, vehicles always have some errors about their locations because of the noise in the environment and sensors. We define the variance of noise as e. Figure. 11 shows that there is an increasing trend in the untraceable quantity as e increases, which is because the noise reduces the accuracy of adversary model.

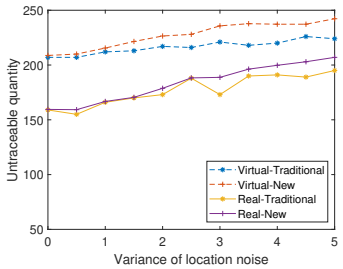

Fig. 11: Influence of e (k=5, p=0, n=4).

VI. CONCLUSION AND FUTURE WORK

In this paper, we review the traditional pseudonym changing methods for privacy protection in VANETs, and propose a

flickering context-based strategy, which takes advantage of the variability of real-time traffic and provided a new perspective for privacy protection. Further, we compare it with the traditional method, and model a global passive adversary to evaluate its performance. The analysis of experimental results show that the proposed strategy performs better than the current context-based method in the terms of entropy and untraceable quantity.

The work presented in this paper leaves some space for further work. For instance, a comparison between different types of strategy, time-based and zone-based has not been conducted, a uniform method or metric is needed to make fair comparison, and the influence of traffic density has not been explored.

VII. Acknowledgment

This research is supported by the National Research Foundation, Prime Ministers Office, Singapore, under its Strategic Capability Research Centres Funding Initiative.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] K. Su, J. Li, and H. Fu, "Smart city and the applications," in *2011 international conference on electronics, communications and control (ICECC)*. IEEE, 2011, pp. 1028–1031.

[3] C. Sommer and F. Dressler, *Vehicular networking*. Cambridge University Press, 2015.

[4] Z. Doukha and S. Moussaoui, "An sdma-based mechanism for accurate and efficient neighborhood-discovery link-layer service," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 603–613, 2015.

[5] H.-J. Lim and T.-M. Chung, "Privacy treat factors for vanet in network layer," in *Soft Computing in Information Communication Technology*. Springer, 2012, pp. 93–98.

[6] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on hot topics in networks (HotNets-IV)*. Maryland, USA, 2005, pp. 1–6.

[7] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[8] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[9] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[10] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *2010 Seventh international conference on wireless on-demand network systems and services (WONS)*. IEEE, 2010, pp. 176–183.

[11] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference, 2005*, vol. 2. IEEE, 2005, pp. 1187–1192.

[12] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," *IEEE Journal on Selected Areas in communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[13] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive computing*, vol. 2, no. 1, pp. 46–55, 2003.

[14] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in vanets," in *2011 IEEE International Conference on Communications (ICC)*. IEEE, 2011, pp. 1–5.

[15] I. Memon, Q. Ali, A. Zubedi, and F. A. Mangi, "Dpmm: dynamic pseudonym-based multiple mix-zones generation for mobile traveler," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 24 359–24 388, 2017.

[16] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *European Workshop on Security in Ad-hoc and Sensor Networks*. Springer, 2007, pp. 129–141.

[17] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *2009 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2009, pp. 1–8.

[18] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in vanets," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 24, no. 1-2, pp. 49–64, 2017.

[19] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Vlpz: The vehicular location privacy zone," *Procedia Computer Science*, vol. 83, pp. 369–376, 2016.

[20] Y. Sun, B. Zhang, B. Zhao, X. Su, and J. Su, "Mix-zones optimal deployment for protecting location privacy in vanet," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1108–1121, 2015.

[21] X. Liu and X. Li, "Privacy preservation using multiple mix zones," in *Location Privacy Protection in Mobile Networks*. Springer, 2013, pp. 5–30.

[22] M. Humbert, M. H. Manshaei, J. Freudiger, and J.-P. Hubaux, "On the optimal placement of mix zones: a game-theoretic approach," in *proceeding of the 16th ACM conference on Computer and Communications Security p*, 2009, pp. 324–337.

[23] M. Gerlach and F. Guttler, "Privacy in vanets using changing pseudonyms-ideal and real," in *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring*. IEEE, 2007, pp. 2521–2525.

[24] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in vanets," in *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*. IEEE, 2009, pp. 648–652.

[25] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2018.

[26] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[27] S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of v2x privacy strategies on intersection collision avoidance systems," in *2013 IEEE Vehicular Networking Conference*. IEEE, 2013, pp. 71–78.

[28] K. Emara, W. Woerndl, and J. Schlichter, "Beacon-based vehicle tracking in vehicular ad-hoc networks," 2013.

[29] J. van Genderen, "Tracking and data fusion: a handbook of algorithms, by yaakov bar-shalom, peter k. willett and xin tian," 2013.

[30] G. Bishop, G. Welch *et al.*, "An introduction to the kalman filter," *Proc of SIGGRAPH, Course*, vol. 8, no. 27599-23175, p. 41, 2001.

[31] R. J. Fitzgerald, "Development of practical pda logic for multitarget tracking by microprocessor," in *1986 American Control Conference*. IEEE, 1986, pp. 889–898.

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

[33] V. Papathanasopoulou, I. Markou, and C. Antoniou, "Online calibration for microscopic traffic simulation and dynamic multi-step prediction of traffic speed," *Transportation research part C: emerging technologies*, vol. 68, pp. 144–159, 2016.

[34] S. Sun, "Optimal and self-tuning information fusion kalman multi-step predictor," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 43, no. 2, pp. 418–427, 2007.

[35] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo–simulation of urban mobility: an overview," in *Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation*. ThinkMind, 2011.

[36] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of sumo-simulation of urban mobility," *International journal on advances in systems and measurements*, vol. 5, no. 3&4, 2012.

[37] S. Buruhanudeen, M. Othman, M. Othman, and B. M. Ali, "Mobility models, broadcasting methods and factors contributing towards the efficiency of the manet routing protocols: Overview," in *2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*. IEEE, 2007, pp. 226–230.