Adjusted Location Privacy Scheme for VANET Safety Applications

Ruqayah Al-ani
Department of Computer Science
Liverpool John Moores University
Liverpool, UK
R.A.AlAni@2015.ljmu.ac.uk

Bo Zhou
Department of Computer Science
Liverpool John Moores University
Liverpool, UK
B.Zhou@ljmu.ac.uk

Qi Shi
Department of Computer Science
Liverpool John Moores University
Liverpool, UK
Q.Shi@ljmu.ac.uk

Thar Baker
Department of Computer Science
Liverpool John Moores University
Liverpool, UK
T.Baker@ljmu.ac.uk

Mohamed Abdlhamed
Imam A'adhum University College
Anbar, Iraq
M.abdalhameed@imamaladham.edu.iq

***Abstract*—The primary aim of Vehicular Ad hoc NETworks (VANET) is to enhance traffic safety by enabling frequent broadcasting of location information between vehicles. In VANET safety applications, a vehicle requires to broadcast messages, which usually contain its location information, every (1-10 Hz) with other vehicles in its communication area (300m) to facilitate cooperative awareness. This would arise privacy issues because vehicles are vulnerable to tracking attacks via their locations. To prevent long-term linking, many privacy schemes have adopted a silent period in which a vehicle stops sharing its locations for a period. However, silent periods could have a negative impact on safety applications as an accident could have happened if a vehicle stop sharing its locations with other neighbours. Thus, in this paper, we first discuss three privacy schemes (RSP, SLOW and CAPS), which adopted silent periods but in different concepts. Then, we improve the privacy and safety level of CAPS. A privacy simulator PREXT is used to evaluate and compare the performance of schemes.**

Keywords—privacy, safety, silent periods, VANET safety applications.

I. INTRODUCTION

Population growth, which could be doubled to 2.5 billion by 2050 [1], has played an important role in the increasing number of traffic on the road. According to the World Health Organization (WHO), nearly 1.35 million people are killed yearly due to traffic road accidents [2].

The development in wireless communications and sensing technologies has encouraged car manufacturers and telecommunication industries to equip vehicles with wireless devices, embedded sensors, and processing capabilities. As a result, vehicles are enabled to collect data about themselves and about their surrounding environment. These data can be exchanged with neighbouring vehicles via a Vehicular Ad hoc NETwork (VANET), which helps in improving road safety [3]. In VANET safety applications, vehicles are required to broadcast messages publicly and periodically at 1-10 Hz in so-called beacon messages. These messages can be received by anyone within the communication range to improve the level of awareness between vehicles such as blind-spot warning, cooperative collision warning, and lane change warning [4].

As the beacon message mainly contains a vehicle's location, speed, and direction, as well as it is broadcasted in plain format, they threatened the privacy of the driver [5]. The eavesdroppers are able to collect and analyze the broadcasted message to track the individual driver's whereabouts by linking subsequent beacons. Therefore, the location privacy of the driver must be protected well prior to the deployment of any VANET applications. An adversary can utilize multi-target tracking techniques to link between messages and track vehicles continuously via its spatiotemporal information [6, 7].

Thus, a vehicle is recommended to stops sharing safety messages (i.e. its location) via entering a silent period. However, VANET safety applications need continuous updating of location information to work properly which could be hindered due to these periods. An acceptable balance between privacy and safety has challenging researchers who have designed privacy schemes depending on silent periods.

Thus, in this paper, three well-known privacy schemes (SLOW [8], RSP [9], and CAPS [10]) have been compared. Then, improving the efficiency of CAPS by adjusting the minimum silent period, which could improve the safety level as well.

The rest of this paper is organized as follows: in section II, we discuss the state-of-the-art schemes that aim to preserve privacy in VANET safety applications. In section III, the system and adversary models are described, and then present the simulation and metrics that are used to collect the achieved results from schemes. Then, in section IV, the performance of the selected schemes is evaluated against our solution. Finally, we show conclusions and future work in section V.

II. RELATED WORK

To meet the public acceptance of any VANET applications, preserving location privacy in VANET has gained significant attention during the past decade. Beresford and Stajano in [11] suggested using mix-zone areas to avoid linkability due to continuous tracking of spatiotemporal information. In mix-zone based scheme, an infrastructure like RSU needs to be installed at intersections or petrol stations. The vehicle would become unobservable when entering these areas to confuse the attacker [12]. However, it is still difficult for vehicles to avoid timing and transition attacks [13] in which attackers can link messages by monitoring enter and exit points of these areas and calculate the time that the vehicle could spend inside them. Moreover, schemes depending on the mix-zone area are required an additional cost to preinstall an infrastructure [14, 15].

Therefore, current standardizations [16] and research efforts have suggested that vehicles can decide locally to be in the unobserved situation by being silent for a period of time. The silent period was first proposed by Huang *et al.* [17] to enhance privacy in wireless networks. Sampigethaya *et al.* [9] were first applied silent periods to VANET in which a vehicle

978-1-7281-4973-8/20/$31.00 ©2020 IEEE

has to choose a Random Silent Period (RSP) between a predefined minimum and maximum values. However, if there is only one vehicle on the road, it would also be identifiable. Thus, Tomandl *et al.* [18] and Li *et al.* [19] suggested that vehicles entering silent periods cooperatively with their neighbours. Moreover, in [19], it is suggested that entering silent periods only when the speed and direction of vehicles are changed. As a vehicle can still be identifiable from its route, Gerlach and Guttler [20] proposed a mix-context approach in which the vehicle being silent for a period cooperatively only if it is surrounding by k-neighbour vehicles who have the same direction and speed.

VANET safety applications need continuous location information updating, silent periods could have a negative impact on their performance, i.e. an accident could be unavoidable. Thus, the scientific challenge is how to balance privacy and safety. In SLOW [8] scheme, authors based on the assumption that the probability of accidents is decreased when the speed of the vehicle is lower than 8m/s [21], the suggestion was allowed for a vehicle to only being silent when its speed is low. However, as the speed of vehicles in the traffic jams are mostly to be low but the probability of accidents is still high; this proves the inefficient of SLOW to be applied to VANET. Emara *et al.* have proposed a Context-Aware Privacy Scheme (CAPS) [10] that reduce silent periods without degrading the privacy level. In CAPS, vehicle cooperatively enters silent period and then resume sending if its context is likely to be mixed with other nearby silent vehicle or being in unobserved locations.

In CAPS, it is suggested that a vehicle need to stop sending messages for a few seconds such as 3s to achieve an acceptable privacy level. However, this assumption is incorrect because a vehicle should start searching for a mix-context with its silent neighbours directly. Waiting for a minimum period could make the vehicle far away from its neighbours (i.e. the cooperative neighbours) which decreases the simultaneous change. Thus, the main aim of this paper is to increase the simultaneous change in CAPS which could improve the privacy level. Moreover, when the vehicle does not obligate to have a minimum silent period, the safety level is probably to be improved because the number of exchanged messages is increased.

III. Methodology

Each vehicle is assumed to be equipped with an OnBoard Unit (OBU) that can store, process, and communicate with other entities. The communications between OBUs/vehicles are wirelessly through Vehicle-to-Vehicle (V2V). In VANET safety applications, a vehicle is required to exchange 10 messages per second with its neighbours within 300 meters. Messages mainly include the vehicle's position, speed, and heading. Moreover, since safety applications require the exact position [22], the vehicle is assumed to be equipped with a GPS receiver.

We test the privacy level of each scheme against a global passive adversary model [23] who eavesdropping and monitoring all broadcasted messages [24]. Then, the ability of the eavesdropper to reconstruct each vehicle traces using multi-target tracking techniques is employed to design a quantitative privacy metric [22]. In [22], the author assumed that the successful eavesdropper has the ability to reconstruct at least 90% of the vehicle's original trace. Then, calculate the average traceability percentage for all vehicles as given in equation (1). The notations used in this paper are illustrated in Table I.

$$Traceabilty = \frac{1}{nV}\sum_{i=1}^{nV} \lambda_i \times 100 \qquad (1)$$

Where

$$\lambda_i = \begin{cases} 1, & \frac{T_i}{vL_i} \geq 90\% \\ 0, & Otherwise \end{cases}$$

Moreover, the safety level is compared by calculating the number of sent messages i.e. higher number indicates less silent period which improves safety. Then, the average number of SBMs for the whole scenario is calculated as given in equation (2) where the value of SBM is 0 when vehicle is silent and 1 when vehicle is active i.e sharing messages.

$$SBMs/s = \frac{1}{vL * nV}\sum_{i=1}^{nV}\sum_{j=1}^{vL}\sum_{k=1}^{br} SBM_i \qquad (2)$$

TABLE I. Notations

Symbol	Stand for	Notation
nV	number of Vehicles	The total number of vehicles generated in SUMO.
vL	Vehicle's Lifetime	The total lifetime of each vehicle as it is arrived and departed at different times.
T_i	Tracking vehicle	The maximum tracking period of vehicle i
MinSP	Minimum Silent Period	Used to enhance privacy.
MaxSP	Maximum Silent Period	Used to decrease the effect on safety.
SBMs	Sent Beacon Messages	The number of sent messages.
m/s	meter per second	Measure the speed of vehicles
br	beacon rates	The number of beacon messages sends every second

To compare between the schemes, we use the PREXT [24] (PRivacy EXTension for veins) simulator, which supports several privacy metrics and schemes. Then, we downloaded the road map area of 3.8 km* 2.8 km of Liverpool/UK using OSM [25], as shown in Fig. 1.

Fig. 1. Road networks downloaded from OSM

IV. Evaluation

First, we run the PREXT simulator based on Adjusted CAPS (ACAPS) in which we assume emitting the minimum silent periods in CAPS [10]. Then, the simulator is run based on the other three privacy schemes (SLOW [8], RSP [9], and CAPS [10]) which applying three different approaches of silent periods. In SLOW, a vehicle stops sharing safety messages as long as its speed less than or equal 8 m/s. In RSP and CAPS, they enforce vehicles to share safety messages for at least 60 s [26] and then enter a silent period. The silent periods should have a minimum (i.e. minimum to meet privacy requirement) and maximum (i.e. to meet application requirement) value such as 3 s and 13 s [27]. Although the silent period in RSP is randomly chosen while in CAPS, the vehicle enters silent cooperatively with its neighbour and keeps silent for 3 s. Then, it starts searching to exit the silent period once its context is probably to be mixed with other silent neighbours or being in an observed position.

To compare the schemes fairly, their parameters are assigned equally whenever possible. Obviously, longer Silent Periods SP would increase tracker confusion thus we assign one values for each parameter i.e. changing SP would have the same impact onto the same scheme. We run each scheme six times with six different vehicle densities for 360s. As a vehicle is required to broadcast safety messages at least 60 s before starting it silent period, the duration of the simulation was chosen equal to 360s (i.e. 6 × 60s) to increase the number of vehicles entering silent period in which more vehicles are participating in the final result. The highest beacon rates for safety applications, which is 10 Hz, is selected to show the worst tracking ratio.

In Fig.2, we compare the privacy level of each scheme via the traceability percentage in equation (1) which is calculated only for vehicles entering the silent period at least once. That is because, in the simulator, a vehicle could have a short lifetime such as less than 60 s (i.e. it has no chance to enter silent) which makes its route traceable while in reality vehicle lifetime i.e. its journey, is properly higher. The safety level for the schemes is calculated using equation (2) as shown in Fig.2 SLOW has scored the worst safety level and the best privacy level, this scheme not suitable for VANET as it contradicts its main aim as nearly 4m/s are missed.

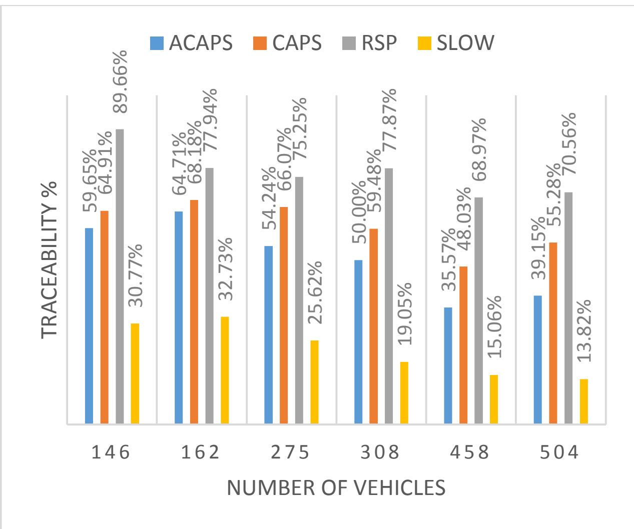

Fig. 2. Traceability

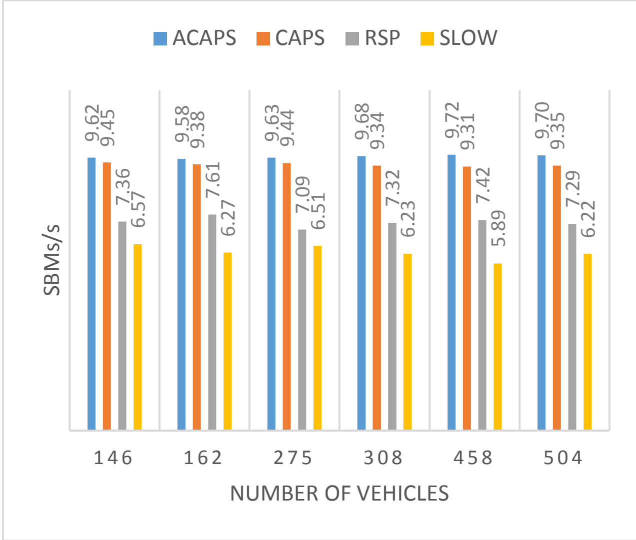

Fig. 3. The Average Number of Safety Messages Sent per Second

Moreover, Fig. 2. has shown that the general trend for the four schemes is that the increase in the density of vehicles enhances privacy as it increases the confusion level of the eavesdropper. As the privacy level of RSP scored the worst which could challenge the public acceptance of VANET applications.

As shown in Fig. 2. ACAPS has achieved the best safety level followed by CAPS as well as ACAPS has enhanced the privacy level of CAPS. For example, in Fig. 2 when vehicle density is 504, ACAPS traceability is 39.15% while in CAPS 55.28% so that privacy is improved significantly by more than 15%. However, the privacy enhancement in ACAPS in comparison to CAPS is started from 3% up to 16% depending on vehicle density as it is difficult for the vehicle to find mix-context with its neighbours in sparse traffic.

V. Conclusions

In this paper, we compare three privacy schemes (CAPS, RSP, and SLOW) which are prevent long-term linkability via applying a silent period but in different concepts. The main aim of this work is to Adjust the minimum silent period in CAPS (ACAPS) which improves the privacy level and decreased the effect on safety. Then, the efficiency of the schemes proved through the PREXT simulator. The results have shown that SLOW has achieved the highest privacy level but it compromises the main aim of VANET i.e. safety via decreasing the exchanged safety messages. RSP has failed to achieve both privacy and safety. CAPS has the least impact on safety in comparison to RSP and SLOW. However, our suggestion in ACAPS has improved the privacy of CAPS up to 15% as well as enhance safety functionality as the number of exchanged messages increased. Thus, we improve the balance between safety and privacy in VANET. For future work, since CAPS and ACAPS have achieved the main aim of VANET, we will continue to improve their privacy level.

References

[1] J. Voelcker, "1.2 Billion Vehicles On World's Roads Now, 2 Billion By 2035," 2014, Available: https://www.greencarreports.com/.

[2] W. H. O. (WHO), "Road traffic injuries," United Nations4 th, 2018, Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries, Accessed on: 13/2/2019.

[3] A. Vaibhav, D. Shukla, S. Das, S. Sahana, and P. Johri, "Security challenges, authentication, application and trust models for vehicular

ad hoc network-a survey," International Journal of Wireless and Microwave Technologies (IJWMT), vol. 7, no. 3, pp. 36-48, 2017.

[4] D. SAE, "J2735 dedicated short range communications (dsrc) message set dictionary," Society of Automotive Engineers, DSRC Committee, 2009.

[5] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," IEEE communications surveys & tutorials, vol. 17, no. 1, pp. 228-255, 2015.

[6] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "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, 2010, pp. 176-183: IEEE.

[7] 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), 2013, pp. 1-6: IEEE.

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

[9] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," Washington Univ Seattle Dept Of Electrical Engineering2005.

[10] K. Emara, W. Woerndl, and J. Schlichter, "CAPS: Context-aware privacy scheme for VANET safety applications," in Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2015, p. 21: ACM.

[11] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on, 2004, pp. 127-131: IEEE.

[12] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "PRIVANET: An efficient pseudonym changing and management framework for vehicular ad-hoc networks," IEEE Transactions on Intelligent Transportation Systems, 2019.

[13] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks," in 2011 IEEE 27th International Conference on Data Engineering, 2011, pp. 494-505: IEEE.

[14] T. Leinmüller et al., "Sevecom-secure vehicle communication," in IST Mobile and Wireless Communication Summit, 2006, no. POST_TALK.

[15] J. Guo and N. Balon, "Vehicular ad hoc networks and dedicated short-range communication," University of Michigan, 2006.

[16] T. ETSI, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," 2018, Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf, Accessed on: 12/6/2019.

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

[18] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in VANETs," in 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2012, pp. 165-172: IEEE.

[19] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in Proceedings of the 5th ACM workshop on Privacy in electronic society, 2006, pp. 19-28: ACM.

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

[21] W. A. Leaf and D. F. Preusser, Literature review on vehicle travel speeds and pedestrian injuries. US Department of Transportation, National Highway Traffic Safety Administration, 1999.

[22] K. A. A. E.-S. Emara, "Safety-aware location privacy in vehicular ad-hoc networks," Technische Universität München, 2016.

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

[24] K. Emara, "Poster: Prext: Privacy extension for veins vanet simulator," in Vehicular Networking Conference (VNC), 2016 IEEE, 2016, pp. 1-2: IEEE.

[25] M. Haklay and P. Weber, "Openstreetmap: User-generated street maps," Ieee Pervas Comput, vol. 7, no. 4, pp. 12-18, 2008.

[26] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, 2009, pp. 1-9: IEEE.

[27] D. Committee, "Dedicated short range communications (DSRC) message set dictionary," Soc. Automotive Eng., Warrendale, PA, USA, Tech. Rep. J2735_200911, 2009.