POSTER: Context-Adaptive User-Centric Privacy Scheme for VANET

Karim Emara[1,2](✉), Wolfgang Woerndl[1], and Johann Schlichter[1]

[1] Department of Informatics, Technical University of Munich (TUM),
Boltzmannstr. 3, 85748 Garching, Germany
{emara,woerndl,schlichter}@in.tum.de

[2] Faculty of Computer and Information Sciences, Ain Shams University,
Khalifa El-Maamon St., Abbasiya, Cairo 11566, Egypt
karim.emara@cis.asu.edu.eg

Abstract. Vehicular adhoc network allows vehicles to exchange their information for safety and traffic efficiency. However, exchanging information may threaten the driver privacy because it includes spatiotemporal information and is broadcast publicly on a periodical basis. In this paper, we propose a context-adaptive privacy scheme which lets a vehicle decide autonomously when to change its pseudonym and how long it should remain silent to ensure unlinkability. This scheme adapts dynamically based on the density of the surrounding traffic and the user privacy preferences. According to the experimental results, the proposed scheme demonstrates a significant reduction in traceability with a better quality of forward collision warning application compared with the random silent period scheme.

Keywords: Context-adaptive privacy · Safety application · Forward collision warning · Random silent period

1 Introduction

Vehicular adhoc networks (VANET) are those networks formed among vehicles and roadside units (RSUs) to provide diverse traffic-related and infotainment applications. VANET is envisioned to enhance traffic safety and efficiency by increasing the awareness of vehicles about their surrounding traffic. To attain this awareness in real-time, vehicles are required to broadcast periodically their current state (i.e., position, speed, heading, etc.) in authenticated *beacon* messages. These messages may threaten the driver location privacy when they are collected by an external eavesdropper because the driver trajectories can be re-identified [1]. There are many privacy schemes that suggest to preload vehicles with a pool of pseudonyms where a single pseudonym is used at a time and changed periodically [7]. However, it is required to change pseudonyms in an unobserved zone in which the adversary cannot monitor the vehicle movements. This zone is often realized by a silent period [8] or in predetermined locations

B. Thuraisingham et al. (Eds.): SecureComm 2015, LNICST 164, pp. 590–593, 2015.
DOI: 10.1007/978-3-319-28865-9_37

(i.e., mix-zone) [6]. The silent period scheme lets a vehicle stop sending messages for a random period before changing its pseudonym. After this period, the vehicle resumes broadcasting beacon messages with a new pseudonym. When it is sufficiently long, a silent period prevents an adversary from tracking vehicle movements and linking old and new pseudonyms but at the cost of safety. Therefore, it is important to consider the impact of a privacy scheme on safety applications to better understand this trade-off between privacy and safety.

In this paper, we propose a context-adaptive privacy scheme (CADS) that utilizes silent period to deliver unlinkability among subsequent pseudonyms. This scheme is a significant improvement of our recent work, context-aware privacy scheme (CAPS) [4]. The CADS minimizes the required parameters by adapting the internal logic according to the density of the surrounding traffic. We integrate also the driver privacy preferences into the scheme to offer privacy constraints only when it is needed by the driver which minimizes the costs on the safety applications.

2 Methodology

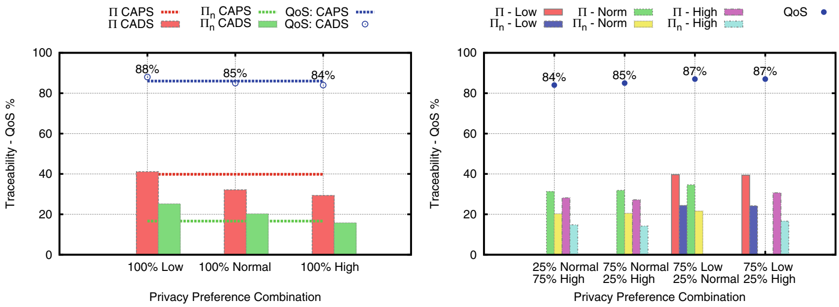
The system and adversary models are assumed to be similar to those proposed in [4]. We used realistic vehicle traces [9] for Cologne city and selected half an hour for the middle 64 km^2 region. The resultant traces are 19,704 where each vehicle appears once with an increasing density ranging from 1,929 to 4,572 simultaneous vehicles in the first and last time steps, respectively. Finally, we add a random noise of 0.5 m to positions.

For privacy evaluation, the vehicle tracker proposed in [2,3] is employed to measure the *traceability* Π of vehicles as explained in [4]. Some vehicles never change their pseudonyms during their lifetime. Thus, the *normalized traceability* Π_n is additionally calculated by excluding these vehicles. For the QoS evaluation of safety applications, we employ our methodology proposed in [5] to evaluate the impact of a privacy scheme on a forward collision warning (FCW) application. In this method, the probability of correctly calculating the main application factors is estimated using Monte Carlo analysis.

3 Context-Adaptive Privacy Scheme (CADS)

The CADS improves the CAPS by allowing a driver to choose low, normal or high privacy preferences. The CADS also minimizes the required parameters by dynamically adapting its context-awareness module according to the density of the surrounding traffic. To optimize the scheme parameters with respect to the surrounding traffic, we investigate the performance of the CAPS in different densities. First, we select two relatively short sub-datasets from the realistic vehicle traces with low and high traffic densities, respectively. Second, the CAPS is evaluated using each sub-dataset with several parameter combinations and obtain the resulting privacy and safety metrics. Third, the results of the sub-dataset experiments are divided into three categories according to the achievable privacy. Fourth, we identify the parameters that result in the best compromise between privacy and safety in each category. Last but not least, these categorized parameters of each density are integrated into CADS and bound according to the real-time vehicle density and the input privacy preference.

The CADS was evaluated in two different scenarios. In the first scenario, all drivers select the same privacy preference whether low, normal or high level. Figure 1(a) displays the Π, Π_n and the QoS of each privacy preference. As a kind of comparison, the measurements for the CAPS scheme of 11 s maximum silent time are shown as dashed lines. The Π and Π_n of CADS decreases when vehicles use a higher privacy level with a concurrent slight decrease in the QoS application. Compared to the CAPS, CADS achieves a better compromise between traceability and QoS.



(a)

(b)

Fig. 1. The CADS evaluation when (a) all vehicles use the same privacy preference compared to the CAPS of 11 s max silent time and (b) vehicles use a random privacy preference based on the specified percentages

In the second scenario, vehicles randomly select the preferred privacy level based on given percentages. The purpose of this scenario is to confirm the enhancement of privacy when some vehicles use a higher privacy level than others. Each experiment is repeated five times using a different random assignment of privacy preferences to vehicles. The mix of low, normal and high privacy preferences for each of the four experiments is specified along the x-axis of Figure 1(b). Although the groups tested in the first two experiments had different percentages of normal and high privacy preferences, we found similar (normalized) traceability achievable by each group in both experiments. Furthermore, the high privacy preference group in the fourth experiment achieves a lower traceability than that achieved by the normal group in the third experiment. Also, the high privacy group in the fourth experiment achieves a higher traceability than that achieved by the same group in the second experiment. This result may attributed to the major privacy preference group being low in the fourth experiment but normal in the second. Regarding the QoS, we notice that it follows the QoS of the major group with a slight effect from the minor. For example, the QoS in the first experiment is the same as that in the 100% high-privacy experiment, and the QoS in the fourth experiment is similar to that in the 100% low-privacy experiment. From all these observations, we can conclude that the traceability is mainly affected by the configured privacy preference with a slight effect from the surrounding traffic. However, this slight change in traceability is compensated positively in the QoS.

4 Conclusion

In this paper, the context-adaptive privacy scheme (CADS) is proposed and evaluated. In CADS, a driver can choose the desired privacy level and the scheme can automatically identify the appropriate parameters that fit this desired level based on the real-time traffic density. Based on the experimental results, CADS reduces traceability than the CAPS does when normal or high privacy levels are selected with a slight reduction in the QoS. In future work, we will compare CADS with advanced privacy schemes such as mix-zones.

References

1. Emara, K.: Location privacy in vehicular networks. In: 2013 IEEE 14th International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–2, June 2013
2. Emara, K., Woerndl, W., Schlichter, J.: Beacon-based Vehicle Tracking in Vehicular Ad-hoc Networks. Tech. rep., TECHNISCHE UNIVERSITÄT MÜNCHEN, April 2013. http://mediatum.ub.tum.de/attfile/1144541/hd2/incoming/2013-Apr/691293.pdf
3. Emara, K., Woerndl, W., Schlichter, J.: Vehicle tracking using vehicular network beacons. In: Fourth International Workshop on Data Security and PrivAcy in wireless Networks 2013 (D-SPAN 2013), Madrid, Spain, June 2013
4. Emara, K., Woerndl, W., Schlichter, J.: Caps: context-aware privacy scheme for vanet safety applications. In: Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec 2015, pp. 21: 1–21: 12. ACM, New York (2015). http://doi.acm.org/10.1145/2766498.2766500
5. Emara, K., Woerndl, W., Schlichter, J.: On evaluation of location privacy preserving schemes for VANET safety applications. Computer Communications **63**, 11–23 (2015)
6. Freudiger, J., Raya, M., Flegyhzi, M., Papadimitratos, P., Hubaux, J.P.: Mix-zones for location privacy in vehicular networks. In: ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), Vancouver, August 2007
7. Petit, J., Schaub, F., Feiri, M., Kargl, F.: Pseudonym Schemes in Vehicular Networks : A Survey. IEEE Communications Surveys & Tutorials (c), 1–31 (2014)
8. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K.: Caravan: providing location privacy for vanet. In: Embedded Security in Cars (ESCAR) (2005)
9. Uppoor, S., Fiore, M.: Vehicular mobility trace of the city of cologne, germany (2011). (accessed January 20, 2015) http://kolntrace.project.citi-lab.fr/