Privacy and Surveillance: Concerns About a Future Transportation System

David Eckhoff
Computer Networks and Communication Systems
Dept. of Computer Science, University of Erlangen, Germany
eckhoff@cs.fau.de

***Abstract*—Intelligent Transportation Systems (ITS) are envisioned as the next step in the evolution of road traffic. They are enablers for visionary technologies such as autonomic driving or traffic light free intersection handling. Furthermore drivers can directly benefit from them in the near future, as they are believed to improve road safety, increase the passengers' comfort and also reduce emissions through dynamic and more accurate route planning. The technology for this is currently being tested and standardized. But what are the drawbacks of such a system? In this article we look into the European and American systems and discuss privacy matters and to what degree they could turn into a surveillance system. We find that the possibilities to do so are manifold and without proper legal and technical aid. Building ITS can very well mean to build the infrastructure to aid an Orwellesque society.**

I. Introduction

According to the World Health Organization there were over 1.2 million road traffic fatalities (and 20-50 million non-fatally injured) in 2009, and even higher numbers have been announced for 2013 [1]. Passive safety systems such as airbags can only reduce this number to a certain degree, making active safety systems such as radars for pre-crash warnings more important.

One promising approach is to enable vehicles to communicate wirelessly to form vehicular networks. The ability of vehicles to communicate with each other and/or the infrastructure allows for many applications to increase road safety in general. By periodically sending the current position, speed, and heading receiving vehicles can automatically detect impending collision and therefore take precautionary steps and warn the driver. While safety is certainly the major advantage of these systems, drivers are envisioned to also benefit from other applications, e.g., dynamic route planning based on information collected by and received from other vehicles or even comfort systems such as video streaming or traffic light assistance systems [2].

Potential downsides of these Intelligent Transportation Systems (ITS) could be insufficient measures to protect drivers' location privacy, i.e., information about current and past whereabouts [3]. This can result to the disclosure of private information and thereby reduce the feeling of freedom of individuals.

It can be argued that it is even possible that these systems allow for overly restrictive law enforcement and thereby even affect the quality of life for the people in it, who may not even have a real choice whether to participate or not. In this article we want to pessimistically discuss possible issues that come with this technology by taking a closer look at the current version of the ETSI and WAVE standards upon which the operation of ITS in Europe, and the USA respectively, will be based.

The remainder of this paper is organized as follows: in Section II we outline why we believe that location privacy is important and is worthy of being protected. We then discuss current approaches and their efficiency as well as their applicability in vehicular networks (Section III). In Section IV we give an outlook on how ITS could be exploited for automated traffic supervision, followed by a discussion about the possibilities to reveal a driver's identity (Section V). We identify open challenges in the field of which we believe – if solved – can substantially help protect drivers' location privacy (Section VI). We conclude this article in Section VII.

II. The Necessity of Location Privacy

Economically, there is a large demand for personal data. Many online services that seem to be free of cost require the individual to disclose personal information in order to work. The users can then evaluate which is more valuable: the data they publish or the benefits they receive from the service, making privacy some kind of currency. So naturally, location privacy has a value attached to it and each person should be able to decide individually what that value is.

While in the industry there is a growing interest to collect personal information in order to generate profit, people seem to accept this and rather pay with their privacy instead of real money. Studies show that location information has only little value to many persons, and a majority of it would sell one month of location data to be used commercially for as little as US$ 35 [4], [5]. Furthermore, the desire of an individual not to be trackable by a third party does not seem to be too big as tracking is already done by mobile phone operators, even though some discuss selling customer location information to retailers.[1] This suggests that from a provider's point of view, preservation of location privacy might not be a critical feature for the design of ITS as it could not even have a significant impact on the financial success.

[1]The Spanish mobile phone operator Telefonica revealed plans to sell customer location information in Spain, England and Germany: http://www.bbc.co.uk/news/technology-19882647

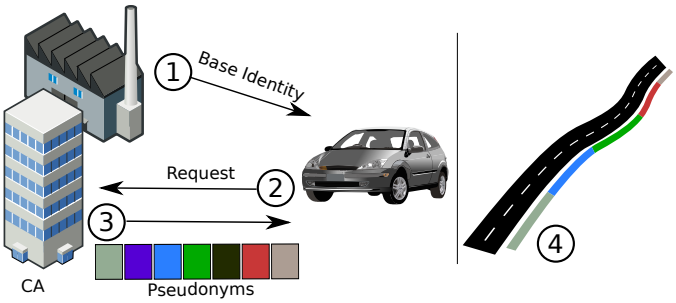

Figure 1. Principles of a PKI in vehicular networks: (1) The vehicle is pre-equipped with a base identity (2) The vehicle requests the signing of pseudonyms (3) The CA signs the pseudonyms if they have been created using the base identity (4) The vehicle uses the pseudonyms as its address.

In many cases, the choice not to use a location based service or to not reveal personal information to some service provider will preserve a user's (location) privacy to a certain degree. There is, however, a difference when it comes to vehicular networks as one of the benefits of these networks is safety, something that most users will probably value higher than location privacy. If ITS do not guarantee location privacy they all but force drivers to trade their location information for the sake of personal safety. This situation becomes worse, when Car-2-Car systems are mandatory for new vehicles as shown by tendencies in current discussions.

A violation of location privacy can lead to unwelcome effects – from obtrusive advertisements to disclosure of information that causes embarrassment or humiliation [6]. This disclosure of a person's location information can lead to the violation of other types of privacy. Knowing an individual visits the hospital three times a week could indicate a medical condition and, for example, make the person less interesting for potential employers. In order to avoid this a system has to provide anonymity, the precondition for location privacy. Anonymity is interpreted by Pfitzmann and Köhntopp [7] as the "state of being not identifiable within a set of subjects [...]". Only when an individual cannot be identified or re-identified, it can preserve its location privacy.

There have been numerous publications on methods and algorithms to preserve location privacy in vehicular networks. As the standardization progresses, it will be interesting to see which approaches will be realized and to what extent location privacy can be protected in ETSI ITS G5 and IEEE WAVE. In the following we examine the current progress and its implications on privacy for drivers. We also discuss how in a worst case scenario a surveillance society may exploit such a system.

III. Location Privacy in Vehicular Networks

In both the European (ETSI ITS G5) and American (IEEE WAVE) systems, all vehicles will periodically emit broadcast messages including information about their current state. A small excerpt from the message format can be found in Table I. The frequency of these messages is envisioned to be at least 1 Hz and at most 20 Hz, depending on the current traffic situation.

Table I
Excerpt from the Cooperative Awareness Message (CAM) [12] and Basic Safety Message (BSM) [13] format

field	comment
direction	direction of the vehicle
position	current (GPS) position
movement	current speed
acceleration	longitudinal and latitudinal acceleration
steeringWheelAngle	(optional) angle of the steering wheel
vehicleLength	length of the vehicle
vehicleWidth	width of the vehicle
exteriorLights	turn signals, headlights, etc.
pathHistory	a history of the last positions

To prevent unauthorized users from joining the network a Public Key Infrastructure (PKI) can be deployed. Vehicles have one pre-installed base identity which must never be used to sign messages, but is only used to generate or request pseudonyms from some kind of (possibly governmental) Certificate Authority (CA). Pseudonyms are also certificates and only valid when signed by the CA. Each vehicle maintains a pool of pseudonyms and uses them as its visible address, that is, to sign and send messages. A message is only valid if it has been signed with a pseudonym that was previously signed by the CA. While it would be beneficial for the anonymity of a driver to use a different pseudonym for each message, it would very likely compromise safety applications of other vehicles, as these can no longer link two messages to the same vehicle. Therefore, pseudonyms are only changed according to some pseudonym change strategy. A common approach is to change the pseudonym from time to time to complicate linking messages with different pseudonyms to each other and hence to prevent the tracking of vehicles.

While this approach does not allow unauthorized users to send valid messages, it does not preclude them from receiving and analyzing this data, because safety messages are not encrypted.

It was shown that pseudonym changes (even with high frequencies of 2 Hz) can be tracked without correlation of additional data [8], if a theoretical attacker was able to overhear all messages. Efficient countermeasures include random silent times, that is, not sending safety messages for a random amount of time after changing a pseudonym [9]. Another approach is context based pseudonym switching, that is, changing pseudonyms when it is believed to cause confusion for possible attacker, e.g. when vehicles with similar states (speed, direction) are close by [10], [11]. However, these approaches possibly interfere with safety applications and are therefore unlikely to be deployed.

Tracking becomes more difficult for an attacker when he is unable to overhear all messages but, for example, only monitors certain areas of a city. Once a vehicle leaves a monitored area and changes its pseudonym before it enters another one, there is good chance to avoid re-identification by an attacker [14]. However, data included in safety messages, such as vehicle

width and height could be used to correlate messages and therefore increase the chance to re-identify a vehicle. The more information a vehicle discloses, the easier it becomes to link two pseudonyms and therefore to track it. It is an open challenge to identify how often and which additional data can be included in messages to avoid this problem and how accurate it has to be to still allow proper operation of safety applications without making vehicles more or less unique. Because even if some data is marked *optional*, the decision whether to include this information will not be made by driver but by the on-board unit.

IV. Automated Surveillance

Even if pseudonyms cannot be linked to each other, the problem remains that each pseudonym can still be resolved to base identities by the authority that signed it, meaning that complete location privacy cannot be ensured.

Although there are different approaches to prevent this (pseudonym swapping [10], blind signatures [15]), they will likely not be a part of future ITS as they possibly violate accountability. It is therefore of utmost importance to lawfully control when and for what cause pseudonyms are allowed to be resolved, for example by the means of knowledge splitting, making it only possible to resolve a pseudonym when multiple institutions cooperate [16].

Accountability in ITS comes with the possibility to resolve a pseudonym to a single unique base identity and thereby to a certain vehicle. Theorteically, this not only allows the identification of vehicles that (deliberately or unintentionally) send false messages, the recovery of stolen vehicles, or the detection of hit-and-run offenses but could also change traffic supervision as we know it.

A vehicle that continuously broadcasts its current velocity will also do so when the driver is speeding. These messages could be received by provider operated road side units for automated ticketing. The formats of safety messages in both ETSI ITS G5 and WAVE make it possible to not only monitor speeding but basically almost all traffic offenses. Turning or lane changing without indication through a turn signal and the violation of traffic lights, right of way or stop lines can all be detected by only evaluating one or few periodic safety messages emitted from a vehicle for example by examining the *exteriorLights*, *pathHistory* or even *steeringWheelAngle* fields.

Tendencies in both academia and industry show that Car-2-X enabled vehicles will be equipped with both ad-hoc 802.11p-based and cellular radio technology, so even in scenarios where no road side unit is nearby to supervise traffic there are possibilities to detect traffic offenses. Receiving vehicles could act as *witnesses* and report traffic offenses directly to some kind of authority over the cellular link. If no cellular connection is available the vehicle could also follow a store-and-forward approach and report to a road-side unit once one is within transmission range. Based on the certainty of the report (potentially derived from the number of vehicles that observed the violation) the misbehaving vehicle could be fined.

We are well aware that from today's view such a scenario certainly seems far-fetched, however, ITS (as currently envisioned) give the operator or the government the ability to deploy these or similar methods in the future. These "features" will most likely not be part of ITS from the beginning, but once on-board-units are widely deployed or even legally mandated, the penetration rate of equipped vehicles will increase – making this kind of traffic supervision far more interesting for certain institutions.

V. Driver Identification

The aforementioned scenarios involve tracking and automated surveillance of vehicles, but not of drivers, that is, individuals. Automated ticketing presumably requires an almost certain identification of the driver or some kind of incontestable proof. Fortunately, this is not a trivial task. However, location information of drivers does not have these strict requirements to be of value. Instead, it suffices if the collected data is likely correct.

Usually, a vehicle is only driven by a very small set of persons, and by only looking at a two week GPS-trace it was shown that, with an accuracy of 60 m, the home address of the driver could be determined, as Krumm showed in 2007 [17]. He also showed that with a simple white page search this was enough to disclose the identity of a driver with an accuracy of 5 %. We expect that with today's presence of social networks this number would be much higher.

With the aid of additional knowledge such as home/work location pairs (city block granularity), Golle et al. were able to identify a large amount ($> 50\,\%$) of drivers [18]. Access to this data is widely available, not only to governmental institutions, but to a variety of parties. Customer location information can be obtained through location based services, social networks, synchronized address books, white pages or public data sets, and even by laws that allow registration offices to sell information on its residents.[2]

The more information can be correlated with a transmitting vehicle, the easier it becomes to identify the actual driver. For example, communicating personal devices such as mobile phones or tablet computers can be traced back to an individual. The use of location based services as well as payment systems that require user identification can also disclose the identity of the driver. More obviously, traffic or surveillance cameras can be directly used to clearly identify a driver and therefore serve as proof that a certain individual was in fact behind the steering wheel.

Lastly, advanced driver assistance systems, including their numerous sensors, are already discussed to be used beyond their main purpose, for example, as a countermeasure against vehicle related crime [19]. In a worst case scenario, fatigue warning systems or dash board cameras could be exploited to

[2] In Germany a law was passed that allows the sale of address data collected at registration offices for commercial purposes: http://www.dw.de/protest-grows-over-german-registration-law/a-16084893

identify drivers and make vehicles support what amounts to automated traffic surveillance.

VI. Open Challenges

In order to build privacy preserving ITS it has first to be fully understood how privacy measures affect other applications such as safety or comfort. Especially the privacy/safety trade-off needs to be investigated more closely to comprehend the exact requirements of safety applications and to draw a reasonable line at the amount and accuracy of information included in periodic safety messages.

On the other hand, it also needs to be easier to evaluate privacy in vehicular networks. Privacy metrics do not only have to be applicable, but also meaningful and easy to understand to allow for the comparison of different approaches, that is, the ability to decide whether one approach is *more private* than another. Furthermore, Open Source simulation frameworks to assess different algorithms are necessary for the integration of privacy methods in future ITS.

Finally, there has to be a stronger emphasis on privacy in ongoing standardization efforts, recommending practices for the technical protection of users' location information and measures to prevent institutions to easily access trusted data and resolve pseudonyms. Retrofitting privacy is bound to fail; therefore field operational tests all over the world should understand privacy as an integral part to serve as an example for future implementations.

VII. Conclusion

Communicating vehicles will change road traffic as we know it and help create Intelligent Transportation Systems. The fact that this technology is mostly beneficial is without controversy; however, certain implications of such a system may raise concerns.

In both ETSI ITS G5 and WAVE vehicles are envisioned to periodically transmit messages containing a considerable amount of information about the vehicle and its current state.

In this paper we showed that this can compromise the location privacy of drivers and that strict legal regulations are needed to control when and by whom this data can be accessed.

Theoretically, these periodic messages could even be used to deploy a fully automated traffic surveillance system and control drivers and vehicles in an overly restrictive fashion. The coverage and accuracy of such a surveillance system could be aided by a high penetration rate and the correlation of data from other systems.

As both families of standards are currently under development, we suggest that these issues are discussed to avoid building an infrastructure that could be exploited in the future. Institutions from both academia and industry should therefore address the open challenges in the field to enable the integration of applicable privacy measures before the roll-out phase, as retrofitting them afterwards is nearly impossible.

References

[1] World Health Organization, "Global Status Report on Road Safety: Time For Action," World Health Organization, Tech. Rep., April 2009. [Online]. Available: http://www.who.int/violence_injury_prevention/road_safety_status/2009/en/

[2] R. Braun, F. Busch, C. Kemper, R. Hildebrandt, F. Weichenmeier, C. Menig, I. Paulus, and R. Presslein-Lehle, "TRAVOLUTION – Netzweite Optimierung der Lichtsignalsteuerung und LSA-Fahrzeug-Kommunikation," *Strassenverkehrstechnik*, vol. 53, pp. 365–374, June 2009.

[3] F. Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks," in *5th International Workshop on Privacy Enhancing Technologies (PET 2005)*, vol. LNCS 3856. Cavtat, Croatia: Springer, May 2005, pp. 197–209.

[4] D. Cvrcek, M. Kumpost, V. Matyas, and G. Danezis, "A study on the Value of Location Privacy," in *13th ACM Conference on Computer and Communications Security (CCS '06). 5th Workshop on Privacy in Electronic Society (WPES)*. Alexandria, VA, USA: ACM, October 2006, pp. 109–118.

[5] G. Danezis, S. Lewis, and R. Anderson, "How Much is Location Privacy Worth?" in *Fourth Workshop on the Economics of Information Security (WEIS'05)*, Cambridge, MA, USA, June 2005.

[6] B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protection," *Computer*, vol. 36, no. 12, pp. 135–137, December 2003.

[7] A. Pfitzmann and M. Köhntopp, "Anonymity, Unobservability, and Pseudonymity - a Proposal for Terminology," in *International Workshop on Design Issues in Anonymity and Unobservability*, ser. LNCS, vol. 2009. Berkeley, CA, USA: Springer, July 2000, pp. 1–9.

[8] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough," in *7th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS 2010)*, Kranjska Gora, Slovenia, February 2010.

[9] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing Wireless Location Privacy Using Silent Period," in *IEEE Wireless Communications and Networking Conference (WCNC 2005)*, New Orleans, LA, March 2005.

[10] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "SlotSwap: Strong and Affordable Location Privacy in Intelligent Transportation Systems," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 126–133, November 2011.

[11] M. Gerlach and F. Guttler, "Privacy in VANETs Using Changing Pseudonyms - Ideal and Real," in *65th IEEE Vehicular Technology Conference (VTC2007-Spring)*, Dublin, Ireland, April 2007, pp. 2521–2525.

[12] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," ETSI, EN 302 637-2 V0.0.9, November 2012.

[13] SAE Int. DSRC Committee, "DSRC Message Communication Minimum Performance Requirements: Basic Safety Message for Vehicle Safety Applications," SAE, Draft Std. J2945.1 Revision 2.2, April 2011.

[14] L. Buttyán, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," in *4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2007)*. Cambridge, UK: Springer, July 2007.

[15] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for Conditional Pseudonymity in VANETs," in *IEEE Wireless Communications and Networking Conference (WCNC 2010)*. Sydney, Australia: IEEE, April 2010.

[16] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure Revocable Anonymous Authenticated Inter-Vehicle Communication (SRAAC)," in *4th Conference on Embedded Security in Cars (ESCAR 2006)*, Berlin, Germany, November 2006.

[17] J. Krumm, "Inference Attacks on Location Tracks," in *5th International Conference on Pervasive Computing (PERVASIVE 2007)*, ser. LNCS, vol. 4480. Toronto, Canada: Springer, May 2007, pp. 127–143.

[18] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," in *7th International Conference on Pervasive Computing*, ser. LNCS, vol. 5538. Nara, Japan: Springer, May 2009, pp. 390–397.

[19] P. Knapik, E. Schoch, M. Müller, and F. Kargl, "Understanding Vehicle Related Crime to Elaborate on Countermeasures based on ADAS and V2X Communication," in *4th IEEE Vehicular Networking Conference (VNC 2012)*. Seoul, Korea: IEEE, November 2012, pp. 86–93.