Safety and Privacy in Vehicular Communications

Josep Domingo-Ferrer and Qianhong Wu

Universitat Rovira i Virgili, UNESCO Chair in Data Privacy, Dept. of Computer Engineering and Mathematics, Av. Països Catalans 26, E-43007 Tarragona, Catalonia
e-mail {josep.domingo,qianhong.wu}@urv.cat

Abstract. Vehicular *ad hoc* networks (VANETs) allow vehicles to disseminate messages about road conditions to other vehicles. As long as these messages are trustworthy, they can greatly increase traffic safety and efficiency. Hence, care must be exerted to ensure that vehicle-generated messages do not convey inaccurate or false content. A natural way to proceed is to request endorsement by nearby vehicles on the content of a message originated by a certain vehicle. However, such a message generation and peer-to-peer endorsement should not result in any privacy loss on the part of vehicles co-operating in it. We survey the available solutions to this security-privacy tension and discuss their limitations. We sketch a new privacy-preserving system which guarantees message authentication through both *a priori* and *a posteriori* countermeasures.

1 Introduction

VANETs allow vehicles to broadcast messages to other vehicles in the vicinity. It is suggested that each vehicle periodically send messages over a single hop every 300ms within a distance of 10s travel time (which is a distance range between 10 m and 300 m)[RH05]. This mechanism can be used to improve safety and optimize traffic. However, malicious vehicles can also make use of this mechanism by sending fraudulent messages for their own profit or just to jeopardize the traffic system. Hence, the system must be designed to ensure that the transmission comes from a trusted source and has not been tampered with since transmission.

Another critical concern in VANETs is driving privacy or vehicle anonymity. As noted in [Dot06], a lot can be inferred on the driver's privacy if the whereabouts and the driving pattern of a car can be tracked. However, it is possible for attackers to trace vehicles by using cameras or physical tracking. But such physical attacks can only trace specific targets and are much more expensive than monitoring the communication in VANETs. This paper addresses the latter attacks.

2 Countermeasures for securing VANETs

VANETs function to improve safety only if the messages sent by vehicles are trustworthy. Dealing with fraudulent messages is a thorny issue for safety engineers due to the self-organized property of VANETs. The situation is deteriorated by the privacy requirements of vehicles since, in a privacy-preserving setting, the message generators, *i.e.* the vehicles, are anonymous in the sense that their identities are unknown. A number of schemes have been proposed to reduce fraudulent messages; such proposals fall into two classes, namely *a posteriori* and *a priori*.

2.1 A posteriori countermeasures

A posteriori countermeasures consist of taking punitive action against vehicles who have been proven to have originated fraudulent messages. To be compatible with privacy preservation, these countermeasures require the presence of a trusted third party able to open the identities of dishonest vehicles. Then the revoked vehicles can be expelled from the system. Cryptographic authentication technologies have been extensively exploited to offer *a posteriori* countermeasures. Some proposals use regular digital signatures [RPH06,RH07,RPAJ07,AFWZ07]. In these proposals, vehicle privacy is provided by a pseudonym mechanism, in which certificate authorities (CAs) produce many pseudonyms for each vehicle so that attackers cannot trace the vehicles producing signatures in different periods with different pseudonyms, except if the CAs open the identities of the vehicles. The pseudonym mechanism is not that efficient due to the heavy overhead of pseudonym generation and storage. Other schemes use sophisticated cryptographic technologies such as group signatures [GBW07] or ring signatures [LSHS07,GGT06]. The latter methods are more efficient, but those using ring signatures cannot trace malicious vehicles due to the unconditional anonymity of ring signatures. Along this research line, the scheme in [GBW07] seems the most efficient one that can provide revokable anonymity.

2.2 A priori countermeasures

A priori countermeasures attempt to prevent the generation of fraudulent messages. This approach is based on the assumption that most users are honest and will not endorse any message containing false data. Another implicit assumption is the usual common sense that, the more people endorse a message, the more trustworthy it is. Along this research

line, the schemes in [GGS04,ODS07,PP05,RAH06,DDSV08] exploit the assumption that there is a majority of honest vehicles in VANETs. Hence, these schemes introduce some form of threshold mechanism: a message is trusted if it has been verifiably endorsed by a number of vehicles above a certain threshold. Among these schemes, the proposals in [DDSV08] may be the most efficient while enabling anonymity of message originators. But their scheme does not provide anonymity revocability, which may not suit some applications in which anonymity must be revoked "for the prevention, investigation, detection and prosecution of serious criminal offences"[EP05].

3 Discussion

Unfortunately, neither *a posteriori* nor *a priori* countermeasures are solely sufficient to secure VANETs. By taking strict punitive action, *a posteriori* countermeasures can exclude some rational attackers producing bogus messages to obtain benefits or pranks. However, they are ineffective against irrational attackers such as terrorists. Even for rational attackers, damage has already occurred when punitive action is taken. It seems that *a priori* countermeasures function better in this case because they prevent damage beforehand by letting the vehicles trust only messages endorsed by a number of vehicles. Although the underlying assumption that there is a majority of honest vehicles in VANETs generally holds, it cannot be excluded that a number of malicious vehicles greater than or equal to the threshold are present in specific locations, for instance. For example, this is very plausible if some criminal organization undertakes to divert traffic from a certain area by broadcasting messages informing that a road is barred. Furthermore, for convenience in implementation, existing schemes use an even stronger assumption that the number of honest vehicles in all cases should be at least a preset threshold. But such a universally valid threshold does not exist in practice. Indeed, the threshold should somehow take the traffic density and the message scope into account: a low density of vehicles calls for a lower threshold, whereas a high density and a message relevant to the whole traffic of a city requires a sufficiently high threshold.

The situation is aggravated by the anonymity technologies used some proposals. A system preserves anonymity when it does not require the identity of its users to be disclosed. Without anonymity, attackers can trace all the vehicles by monitoring the communication in VANETs, which in turn can enable the attackers to mount serious attacks against specific

targets. Hence, anonymity is a critical concern in VANETs. However, anonymity can also weaken *a posteriori* and *a priori* countermeasures. Indeed, attackers can send fraudulent messages without fear of being caught due to anonymity, and as a result, no punitive action can be taken against them. Furthermore, some proposals provide strong anonymity, *i.e.* unlinkability. Unlinkability implies that a verifier cannot distinguish whether two signatures come from the same vehicle or two vehicles. This feature may enable malicious vehicles to mount the so-called Sybil attack: a vehicle generates a fraudulent message and then endorses the message herself by computing on it as many signatures as required by the threshold in use; since signatures are unlinkable, no one can find out that all of them come from the same vehicle. Hence, elegantly designed protocols are required to secure VANETs when incorporating anonymity.

4 Towards a combination of *a priori* and *a posteriori* countermeasures

Bearing in mind that enhancing safety and traffic efficiency is one of the main thrusts behind VANETs, we propose a new efficient system to balance public safety and vehicle privacy. Both *a priori* and *a posteriori* countermeasures are resorted to in order to thwart attackers. To the best of our knowledge, ours is the first system equipped with both types of countermeasures. We achieve this goal by drawing on the novel technology of message-linkable group signatures (MLGS). In an MLGS scheme, a vehicle stays anonymous if it produces two signatures on two different messages. However, if it produces two signatures on the same message, then it will be identified, which effectively thwarts the Sybil attack in a privacy-preserving system. This novel technology also enables us to realize a threshold-adaptive authentication in which the threshold can adaptively change in light of the context of messages, instead of having to be preset during the system design stage. Furthermore, a fast batch verification method is presented to speed up the validation of authenticated messages. Since vehicles periodically receive a large number of messages to be validated, such a batch verification is critical to make authentication implementable in VANETs. Details on the new scheme will be given in [WD08].

Acknowledgments and disclaimer

This work was partly supported by the Spanish Government through projects CONSOLIDER INGENIO 2010 CSD2007-00004 “ARES” and

TSI2007-65406-C03-01 “E-AEGIS”, and by the Government of Catalonia under grant 2005 SGR 00446. The authors are with the UNESCO Chair in Data Privacy, but their views do not necessarily reflect the position of UNESCO nor commit that organization.

References

[RH05] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In SASN'05, 2005.

[Dot06] F. Dötzer. Privacy issues in vehicular ad hoc networks. Lecture Notes in Computer Science, vol. 3856, pp. 197-209, 2006.

[RPH06] M. Raya, P. Papadimitratos and J.-P. Hubaux. Securing vehicular communications. IEEE Wireless Communications Magazine, vol. 13, no. 5, pp. 8-15, 2006.

[RH07] M. Raya and J.-P. Hubaux. Securing vehicular ad hoc networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 39-68, 2007.

[RPAJ07] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J.-P. Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557-1568, 2007.

[AFWZ07] F. Armknecht, A. Festag, D. Westhoff and K. Zeng. Cross-layer privacy enhancement and non-repudiation in vehicular communication. In 4th Workshop on Mobile Ad-Hoc Networks (WMAN), Bern, Switzerland, March 2007.

[GBW07] J. Guo, J.P. Baugh and S. Wang. A group signature based secure and privacy-preserving vehicular communication framework. In Mobile Networking for Vehicular Environments, pp. 103-108, 2007.

[LSHS07] X. Lin, X. Sun, P.-H. Ho and X. Shen. GSIS: A secure and privacy preserving protocol for vehicular communications. IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, 2007.

[GGT06] C. Gamage, B. Gras and A.S. Tanenbaum. An identity-based ring signature scheme with enhanced privacy. In Proceedings of the IEEE SecureComm Conference, pp. 1-5, 2006.

[GGS04] P. Golle, D. Greene and J. Staddon. Detecting and correcting malicious data in VANETs. In Proceedings of the 1st ACM international workshop on Vehicular Ad Hoc Networks, pp. 29-37, 2004.

[PP05] B. Parno and A. Perrig. Challenges in securing vehicular networks. In Proceedings of the ACM Workshop on Hot Topics in Networks, 2005.

[ODS07] B. Ostermaier, F. Dötzer and M. Strassberger. Enhancing the security of local danger warnings in VANETs - A simulative analysis of voting schemes. In Proceedings of the Second International Conference on Availability, Reliability and Security, pp. 422-431, 2007.

[RAH06] M. Raya, A. Aziz and J.-P. Hubaux. Efficient secure aggregation in VANETs. In Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks - VANET 06, pp. 67-75, 2006.

[DDSV08] V. Daza, J. Domingo-Ferrer, F. Sebe and A. Viejo. Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, Accepted, July 2008.

[EP05] European Parliament. Legislative resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data

processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 C6-0293/2005 2005/0182(COD)), 2005

[WD08] Q. Wu and J. Domingo-Ferrer. Improved trustworthiness of vehicular communications with a priori and a posteriori countermeasures. Manuscript in preparation, 2008.