A Cooperative Location Privacy Protection Scheme for Vehicular Ad-hoc Networks

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology, Stockholm, Sweden
{*khodaei, papadim*}@kth.se

The concept of smart cities is shaping future urban infrastructure and influences transportation systems. Smart vehicles, as the principal building block of Intelligent Transport Systems (ITSs), are on the way and car-makers are mandated to equip vehicles with new communication technologies. Meanwhile, Field Operational Testing (FOT) for self-driving cars is on-going. These set the ground for the emergence of innovative applications to improve road safety, transportation efficiency, environmental hazards and driving experience. Vehicles are to be provided with special-purpose sensors and equipment to monitor their operation and surroundings; On-Board Units (OBUs) facilitate Dedicated Short Range Communication (DSRC), over ITS-G5 (i.e., IEEE 802.11p) or leverage the cellular infrastructure for communicating with other OBUs or Roadside Units (RSUs). Vehicles periodically disseminate Cooperative Awareness Messages (CAMs) about their actions and whereabouts containing location, velocity, and acceleration. Thus, neighboring vehicles will be informed about possible unexpected incidents or objects beyond their sight, e.g., *motorcycle approaching indication* as a typical safety application.

Such a large-scale Vehicular Communication (VC) system cannot materialize unless the VCs are secure and do not expose users' (drivers and passangers) privacy. There is a growing consensus towards deploying a special-purpose identity and credential management infrastructure, i.e., a Vehicular Public-Key Infrastructure (VPKI), e.g., [1, 2, 3, 4, 5, 6, 7, 8]: a set of Certification Authorities (CAs) provide anonymized certificates, *pseudonyms*, to the legitimate vehicles. However, due to the openness of the wireless communication, an eavesdropping observer could infer sensitive information. For location privacy, there are different solutions: *K-anonymity* ensures that a target node is not distinguishable from at least $K-1$ nodes within the *anonymity set* with respect to the information each node disseminates, e.g., location and velocity. However, not all the nodes in the anonymity set may be equally likely to be targeted: an adversary could obtain additional information about a target node towards predicting its movement and trajectory. Relying on group signature schemes to enhance user privacy also would degrade the performance of the safety-related applications [9].

Pseudonymous authentication is a promising approach to protect user privacy; however, an adversary eavesdropping all traffic in an area could link successive pseudonymously authenticated messages. More precisely, an adversary might observe an isolated pseudonym change, and associate the old and new pseudonymous identifiers through *syntactic linking*, e.g., [10]. While appropriate pseudonym provisioning policies alleviate syntactic linking attacks through issuing pseudonyms with time-aligned lifetimes [2, 3, 5], compromising user privacy by conducting *semantic linking* attacks is still feasible: an adversary could leverage physical constraints of the road layout, and message payload, e.g., location, velocity, time, of a victim's vehicle to predict its trajectory towards linking messages *semantically*.

In this poster, we show how one can classify vehicles based on the information (CAMs) they carry towards conducting semantic linking attacks. Such information could be unique, or one of few, and thus, can be easily linked by an external observer. We propose a novel user-centric mix-zone scheme to be resilient against syntactic and semantic linking attacks. Our scheme also maintains strong user privacy protection for vehicles upon pseudonym change in the presence of *honest-but-curious* system entities. Moreover, our scheme is resilient against internal adversaries, i.e., faulty or malicious vehicles, that try to degrade the anonymity set.

REFERENCES

[1] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, ''A Security Credential Management System for V2V Communications,'' in *IEEE VNC*, Boston, MA, Dec. 2013.

[2] M. Khodaei, H. Jin, and P. Papadimitratos, ''Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,'' in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[3] M. Khodaei and P. Papadimitratos, ''The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,'' *IEEE VT Magazine*, vol. 10, no. 4, pp. 63--69, Dec. 2015.

[4] ------, ''Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,'' in *IoV/VoI*, Paderborn, Germany, July 2016.

[5] M. Khodaei, H. Jin, and P. Papadimitratos, ''SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,'' *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 5, pp. 1430--1444, May 2018.

[6] M. Khodaei and P. Papadimitratos, ''Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs,'' in *ACM WiSec*, Stockholm, Sweden, June 2018.

[7] H. Noroozi, M. Khodaei, and P. Papadimitratos, ''DEMO: VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure,'' in *ACM WiSec*, Stockholm, Sweden, June 2018.

[8] M. Khodaei, H. Noroozi, and P. Papadimitratos, ''Scaling Pseudonymous Authentication for Large Mobile Systems,'' in *ACM WiSec*, Miami, FL, USA, May 2019.

[9] M. Khodaei, A. Messing, and P. Papadimitratos, ''RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd,'' in *IEEE VNC*, Torino, Italy, Nov. 2017.

[10] M. Khodaei, H. Noroozi, and P. Papadimitratos, ''POSTER: Privacy Preservation through Uniformity,'' in *ACM WiSec*, Stockholm, Sweden, June 2018, pp. 279--280.