Poster: Mix-Zones Everywhere: A Dynamic Cooperative Location Privacy Protection Scheme

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

***Abstract*—Inter-vehicle communications disclose rich information about vehicle whereabouts. Pseudonymous authentication secures communication while enhancing user privacy. To enhance location privacy, cryptographic mix-zones are proposed where vehicles can covertly update their credentials. But, the resilience of such schemes against linking attacks highly depends on the geometry of the mix-zones, mobility patterns, vehicle density, and arrival rates. In this poster, we propose *"mix-zones everywhere"*, a cooperative location privacy protection scheme to mitigate linking attacks during pseudonym transition. Time-aligned pseudonyms are issued for all vehicles to facilitate *synchronous* pseudonym updates. Our scheme thwarts Sybil-based misbehavior, strongly maintains user privacy in the presence of *honest-but-curious* system entities, and is resilient against misbehaving insiders.**

I. Introduction

In Vehicular Communication (VC) systems, vehicles disseminate Cooperative Awareness Messages (CAMs) periodically at a high rate. Vehicular communication, including CAMs, is secured: a set of short-term anonymous credentials, i.e., *pseudonyms*, are provided to each vehicle by the Vehicular Public-Key Infrastructure (VPKI) [1], [2]. Vehicles switch from one pseudonym to another for message unlinkability.

Due to the openness of the wireless communication in VC systems, an observer could eavesdrop towards inferring vehicle-sensitive information. Although pseudonymous authentication is a promising approach to protect user privacy, an adversary, eavesdropping all traffic in an area, could link successive pseudonymously authenticated messages. More precisely, an attacker could link successive CAMs by attempting to *syntactically* link the corresponding pseudonym with the same identifier [3], or *semantically* link the message using their payload, e.g., time, location, and velocity [4], [5].

Cryptographic Mix-Zone-based schemes [6] were proposed to establish a cryptographically protected region at appropriate times and places, e.g., at intersections. All legitimate vehicles within the mix-zone receive a symmetric session key from a Roadside Unit (RSU), responsible for the initiation of pseudonym transition process and symmetric key updates [6]. Vehicles encrypt CAMs and opt in updating their pseudonyms while crossing these regions. The achieved privacy protection level for such statically constructed mix-zones highly depends on the geometry of mix-zones, mobility pattern and arrival rates. For example, based on the mix-zone geometries [7], or the traffic mobility pattern and vehicle speed [5], [6], [8], [9], an adversary can link successive pseudonyms of a given vehicle by observing the mix-zone entry and exit points.

Alternatively, vehicles could participate to form a dynamic mix-zone, e.g., [10]: each On-Board Unit (OBU) is provided with a global symmetric key, using it to initiate a pseudonym change process. However, an internal attacker could terminate the encryption period on behalf of any vehicle, thus degrading down the anonymity set. Beyond significant overhead in key management, i.e., distributing a new key to all vehicles upon a revocation event, this scheme requires that vehicles change speed and lane or direction when updating their pseudonyms; thus, the practicality of such a scheme is questionable.

The common denominator among most of the prior proposals is that vehicles are provided with multiple valid pseudonyms at any given point in time. This is indeed necessary to reach a mix-zone and initiate the pseudonym transition process. However, this sets the ground for Sybil-based misbehavior (note that a Hardware Security Module (HSM), ensuring all signatures are generated under a single valid pseudonym at any time, can be a general remedy). Unlike all such systems, our scheme mitigates syntactic and semantic linking attacks while thwarting Sybil-based misbehavior. Moreover, prior works assume that the system entities are fully trustworthy, e.g., RSUs and VPKI entities could link successive pseudonyms belonging to a given vehicle. However, recent revelations of mass surveillance show that assuming service providers are fully-trustworthy is no longer a viable approach. Our scheme 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 down the anonymity set of other vehicles by not changing their pseudonyms.

II. System and Adversarial Model

We assume a VPKI with distinct entities and roles that registers vehicles in a domain [11] and issues pseudonyms [1], [2], [12]. To achieve full unlinkability, a universally fixed interval is specified and all pseudonyms are issued with the lifetime aligned with the VPKI clock. In case of any deviation, the misbehaving entities should be evicted and revocation information are distributed [13]. All vehicles are provided with HSMs, ensuring that private keys never leave the HSM. The certificates of higher-level authorities are installed on the OBUs, loosely synchronized with the VPKI servers. We further assume that appropriate countermeasures are in place to prevent from location spoofing, e.g., [14], enable secure neighborhood discovery [15], and facilitate physical position verification [16].

External adversaries could eavesdrop VC systems to infer user-sensitive information to harm user privacy. Internal adversaries could affect the operation of our scheme in four ways: (i) initiating the protocol continuously to impose extra overhead on the VC systems, (ii) terminating the protocol to degrade down the anonymity set, and (iii) opt in not changing their pseudonyms to degrade down the anonymity set. Further, adversaries could also (iv) collude and share information that each of them individually collected to compromise user privacy. For example, RSUs could share a transcript of pseudonymously authenticated messages with an *honest-but-curious* VPKI entity [2] towards harming user privacy.

III. Mix-Zones Everywhere

Upon reaching a pseudonym transition process, a dynamic mix-zone formation is initiated by a vehicle and all CAMs within each mix-zone are encrypted using a distinct symmetric session key. Protocol 1 shows the initiation process of a mix-zone: when the current pseudonym is expiring, a vehicle initiates the mix-zone formation. It explicitly sets the *INIT-MIX* flag in the upcoming CAMs to inform their neighbors (steps 2–5). It then generates a symmetric key (step 6), encrypts it with the public keys of its neighboring vehicles, and signs the message before broadcasting (steps 7–13). The termination process is as follows: vehicles vote to terminate the encrypted communication when sufficiently many changes, e.g., lane, speed, and direction, were detected. Distributing symmetric keys and establishing a cryptographically protected communication could incur extra computation and communication overhead; but, given the data-rates up to 24 Mbit/s and available computing resources, it will not create significant overhead on the VC system. For example, Nexcom boxes from the PRESERVE project (goo.gl/m8kjtg), are capable of computing 6,742 ECDSA signatures and 2,780 verifications per second.

IV. Security & Privacy Analysis

The VPKI [1], [2] issues the pseudonyms with non-overlapping lifetimes and no vehicle can obtain more than one valid pseudonym at any time, thus mitigating Sybil attacks. The VPKI can be configured to issue fully unlinkable pseudonyms [2], [12]; by colluding RSUs and VPKI entities, one cannot infer information upon pseudonym change to harm user privacy because the entire communication is cryptographically protected. Moreover, malicious internal vehicles could collude with an RSU or a VPKI entity; however, due to the dynamic formation of mix-zones and fully-unlinkable pseudonyms, no user-sensitive information is disclosed to harm user privacy. Moreover, malicious internal vehicles cannot initiate or terminate the protocol at any time, nor ignoring changing their pseudonyms because each vehicle has only one valid pseudonym and it must change to the next one.

Issuing pseudonyms with non-overlapping intervals mandates vehicles to change their pseudonyms when current pseudonym lifetime expires. Thus, in a low traffic density area where there are very few vehicles to cooperatively change pseudonyms, vehicles could be *semantically* linkable. If vehicles could have opted in not changing their pseudonyms in such circumstances, they would be *trivially* linkable. Thus, issuing pseudonyms with non-overlapping intervals does not degrade user privacy.

Protocol 1: Mix-Zone Initiation Protocol

1: **procedure** INITIATE-MIXZONE()
2: $Flag_{INIT\text{-}MIX} \leftarrow True$ ▷ Initializing Mix-zone flag to true
3: $CAM \leftarrow \{Fields, Flag_{INIT\text{-}MIX}, t_{now}\}$ ▷ Encapsulating a CAM
4: $(CAM)_{\sigma_{k_v}} \leftarrow \text{Sign}(CAM, K_v)$ ▷ Signing the CAM
5: $broadcast((CAM)_{\sigma_{k_v}})$ ▷ Broadcasting a CAM with Mix-zone initiation
6: Generate(SK) ▷ Generating a symmetric key SK
7: **for** i:=1 to **n do** ▷ n: number of neighboring vehicles
8: **Begin**
9: $SK_{\sigma_{K_v^i}} \leftarrow \text{Encrypt}(K_v^i, SK)$ ▷ Encrypting SK with a neighbor's public key
10: $\zeta \leftarrow (INIT\text{-}MIX, SK_{\sigma_{K_v^i}}, K_v, K_v^i, t_{now})$ ▷ Encapsulating the msg
11: $\zeta_{\sigma_{k_v}} \leftarrow Sign(k_v, \zeta)$ ▷ Signing the message with it's private key
12: $broadcast(\zeta_{\sigma_{k_v}})$ ▷ Broadcasting Mix-zone SK
13: **End**
14: **end procedure**

V. Conclusion and Future Work

We demonstrate a cooperative formation of mix-zone to enhance location privacy. As future work, we plan to gauge the performance and achieved privacy protection of our scheme.

Acknowledgement

This work has been partially supported by the Swedish Foundation for Strategic Research (SSF) SURPRISE project.

References

[1] 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.

[2] M. Khodaei *et al.*, "SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems," *IEEE T-ITS*, vol. 19, no. 5, pp. 1430–1444, May 2018.

[3] ——, "POSTER: Privacy Preservation through Uniformity," in *ACM WiSec*, Stockholm, Sweden, June 2018, pp. 279–280.

[4] L. Buttyán *et al.*, "SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs," *IEEE VNC*, Oct. 2009.

[5] B. Wiedersheim *et al.*, "Privacy in Inter-vehicular Networks: Why Simple Pseudonym Change is not Enough," in *WONS*, KG, Slovenia, Feb. 2010.

[6] J. Freudiger *et al.*, "Mix-zones for Location Privacy in Vehicular Networks," in *Win-ITS*, Vancouver, BC, Canada, Aug. 2007.

[7] B. Palanisamy and L. Liu, "Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms," *IEEE TMC*, vol. 14, no. 3, pp. 495–508, Mar. 2015.

[8] J. Krumm, "Inference Attacks on Location Tracks," in *International Conference on Pervasive Computing*, Toronto, Canada, May 2007.

[9] A. Tomandl *et al.*, "Simulation-based Evaluation of Techniques for Privacy Protection in VANETs," in *WiMob*, Barcelona, Spain, Oct. 2012.

[10] A. Wasef and X. Shen, "REP: Location Privacy for VANETs Using Random Encryption Periods," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 172–185, Feb. 2010.

[11] 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.

[12] M. Khodaei *et al.*, "Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems," in *Proceedings of the IoV-VoI*, Paderborn, Germany, pp. 7–12, July 2016.

[13] M. Khodaei and P. Papadimitratos, "Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs," in *ACM WiSec*, Stockholm, Sweden, June 2018, pp. 172–183.

[14] P. Papadimitratos and A. Jovanovic, "GNSS-based Positioning: Attacks and Countermeasures," in *IEEE MILCOM*, San Diego, CA, USA.

[15] P. Papadimitratos *et al.*, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, Feb. 2008.

[16] M. Fiore *et al.*, "Discovery and verification of neighbor positions in mobile ad hoc networks," *IEEE TMC*, vol. 12, no. 2, pp. 289–303, Feb. 2013.