POSTER: Increasing Mix-Zone Efficacy for Pseudonym Change in VANETs using Chaff Messages

Christian Vaas
University of Oxford
Oxford, United Kingdom
christian.vaas@cs.ox.ac.uk

Panos Papadimitratos
KTH Royal Institute of Technology
Stockholm, Sweden
papadim@kth.se

Ivan Martinovic
University of Oxford
Oxford, United Kingdom
ivan.martinovic@cs.ox.ac.uk

ABSTRACT

Vehicular ad-hoc networks (VANETs) are designed to play a key role in the development of future transportation systems. Although cooperative awareness messages provide the required situational awareness for new safety and efficiency applications, they also introduce a new attack vector to compromise privacy. The use of ephemeral credentials called *pseudonyms* for privacy protection was proposed while ensuring the required security properties. In order to prevent an attacker from linking old to new pseudonyms, mix-zones provide a region in which vehicles can covertly change their signing material. In this poster, we extend the idea of mix-zones to mitigate pseudonym linking attacks with a mechanism inspired by chaff-based privacy defense techniques for mix-networks. By providing chaff trajectories, our system restores the efficacy of mix-zones to compensate for a lack of vehicles available to participate in the mixing procedure. Our simulation results of a realistic traffic scenario show that a significant improvement is possible.

1 INTRODUCTION

Vehicular ad-hoc networks (VANETs) are designed to play a key role in the development of future transportation systems. Through vehicle-to-vehicle communication, these networks provide situational awareness allowing the implementation of new transportation safety and efficiency applications. To achieve this, vehicles' on-board units (OBUs) periodically broadcast Cooperative Awareness Messages (CAMs) that inform other vehicles about their exact location and velocity in real time. The authenticity, integrity, and non-repudiation of messages is ensured using digital signatures and public key cryptography. Each OBU receives an individual public and private key, issued by a central certification authority (CA) that can be resolved to the identity of the vehicle owner.

Although a person's identity can only be revealed by the CA, using static credentials for signature generation still allows an attacker to compromise the passengers' privacy. For example, by linking consecutive messages, a passive adversary can track vehicles and even infer the identity of the driver [1]. As a solution, ephemeral credentials called *pseudonyms* were proposed for privacy preservation [5]. By changing to a fresh pseudonym, these schemes aim to break the trip of a vehicle down into smaller unlinkable segments. Despite the theoretical feasibility of such approaches, two categories of attacks, semantic and syntactic linking were identified [2]. Both exploit the context in which vehicles change their pseudonym. Syntactic linking occurs when the attacker observers isolated pseudonym changes that make associating the new and old identifier easy. During a semantic linking attack, the adversary makes use of the physical constraints given by the road layout, velocity, and direction of the observed vehicles to predict a vehicle's trajectory. Based on CAM content, this eventually allows the attacker to link consecutive pseudonyms.

Appropriate pseudonym provision policies, with time aligned and short credential lifetimes, can greatly alleviate syntactic linking [6]. But semantic linking requires additional countermeasures. Based on the idea of network mixes, to protect anonymity in computer networks, Freudiger et al. [4] transferred this approach to VANETs. Their construction of cryptographic mix-zones (CMIX) provides protected road segments at intersections in which vehicles can jointly change pseudonyms and physically mix to prevent semantic linking attacks.

In this poster, we investigate the impact of traffic demand, that is the availability of vehicles to participate in a mix-zone on its efficacy. After identifying that the performance of mix-zones suffers under low-traffic conditions, we propose the use of chaff messages to counteract this issue. These messages mimic real vehicles to conceal when a vehicle exists a mix-zone and hence protect against semantic linking attacks. To measure the performance of our system, we put forward a new metric for privacy loss based on an attacker's probability to compromise a vehicle's journey. Finally, we evaluate the computation overhead and privacy increase by performing simulations of realistic road traffic.

2 OUR APPROACH

We start the presentation of our approach with preliminaries on the adversary model and chaff messages followed by the details of our scheme and the evaluation setting.

2.1 Preliminaries

Adversary. We consider a passive external adversary with wireless eavesdropping capabilities, observing vehicles entering and exiting mix-zones via receivers placed next to road intersections. The attacker is not in possession of valid credentials and therefore cannot obtain the symmetric key used within the mix-zone. As a result, it can only receive CAMs of vehicles entering and leaving the mix-zones but cannot decrypt messages from within the mix-zone. The goal of the attacker is to compromise the location privacy of vehicles by finding a mapping between the old and new pseudonyms

WiSec '18, Stockholm, Sweden

978-1-4503-5731-9/18/06…$15.00
DOI: 10.1145/3212480.3226103

of a vehicle. To achieve this, the attacker, first, characterizes the pairwise probabilities between adjacent lanes, i.e., how likely it is that a vehicle exits at lane *A* given that it entered through lane *B*. Secondly, it creates a model of the mix-zone traversal delay, as a function of the road layout. That is, given the time a vehicle spent in the mix-zone, pairs of entry and exit lanes can be ranked by likelihood of being taken by the victim.

Chaff Messages. Chaff-based defenses have been used to prevent traffic analysis in computer networks and provide anonymous communication. These use indistinguishable fake messages to conceal differences in transmission rates such that every network node exposes the same rate. In a mix-zone network, messages are equivalent to vehicles traversing the roads. Differences in arrival times and traffic density allow traffic analysis to track vehicles across pseudonym changes. A lack of traffic participants increases the chances of a successful attack, hence inserting vehicles into the traffic flow leads to an effect similar to chaff messages.

2.2 Details

We enhance the mix-zone functionality by authorize the RSUs that instantiate the cryptographic mix-zone to obtain additional pseudonym sets. These are uniquely used for the generation of chaff CAMs to make up for a lack of participants in a mix-zone. We assume that each OBU is provisioned with a set of pseudonyms with non-overlapping lifetimes, meaning a vehicle has only one active pseudonym at a time. Mix-zones are located at intersections where a RSU provides a symmetric key to each vehicle for message encryption. For chaff vehicle trace generation, a RSU computes all possible trajectories of a vehicle when it enters the mix-zone. These vehicle traces are compared to those of other vehicles passing through the intersection to prevent conflicts, i.e., collisions. The resulting set of traces combined with CAM information from real vehicles is used to derive actual chaff CAMs. To ensure that an observing adversary cannot differentiate between chaff and real awareness messages, RSUs maintain a pool of chaff credentials that allow produced signatures to be validated against the CA. Finally, the chaff messages that include location information situated within its transmission range are disseminated by the RSU directly, while messages containing locations further away need to be delegated to adjacent vehicles which function as relays. In order to alleviate the computational overhead caused when receiving caff messages, vehicles within the mix-zone are provided with a set of chaff certificate hashes. When receiving a CAM, vehicles that participated in the mix-zone can perform a membership test of the attached certificate against the provided set and discard them accordingly.

3 EVALUATION

We implemented our protocol to evaluate its performance in a simulation with realistic vehicle traffic. The LuST project [3] provides 24 hours of vehicle trajectories within the road network of the city of Luxembourg. Based on this, we use the SUMO simulation framework to place mix-zones at each intersection of the road network. We simulate an attacker with varying resources following four different strategies to select a set of mix-zones to observe. To compute the level of privacy compromise for a trip, the road network is represented as graph as defined in Equation 1. A trip T's length is given as described in Equation 2 which enables to compute the privacy compromise *P(T)* as the trip's segments weighted with the attacker's probability *p(a,b)* that a vehicle coming from node a transitions to node b when passing the mix-zone, see Equation 3.

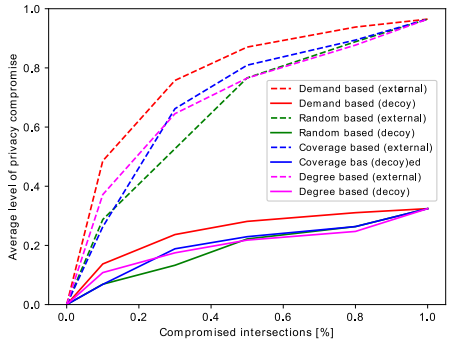

Figure 1: Average level of privacy compromise with respect to the percentage of intersections observed by the attacker. Intersections are chosen using four different strategies.

$$G = (N, E) \mid N = Nodes; E = (a, b) \mid a, b \in N \tag{1}$$

$$l : E \rightarrow \mathbb{N}; T = E^n; |T| = \sum_{i=0}^{n} l(e_i) \mid e_i \in T \tag{2}$$

$$P(T) = \frac{\sum_{i=0}^{n} l(e_i) * p(a,b)}{|T|} \mid (a,b) = e_i;\ e_i \in T \tag{3}$$

To establish a baseline, we use this metric to compare the mix-zone network under ideal traffic to realistic traffic demand and show that a lack of vehicles reduces the efficacy of this approach. We then repeat the simulations using our extended mix-zone protocol. As shown in Figure 1, our scheme significantly improves from the realistic traffic scenario by adding chaff messages. Dashed lines denote the original CMIX protocol under realistic traffic, while solid lines denote our extended protocol.

REFERENCES

[1] Jacob Bellatti and Andrew Brunner. 2017. Driving Habits Data : Location Privacy Implications and Solutions. *IEEE Security & Privacy* (2017), 12–20.
[2] Abdelwahab Boualouache, Sidi Mohammed Senouci, and Samira Moussaoui. 2017. A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks. *IEEE Communications Surveys and Tutorials* (2017), 1–25.
[3] Lara Codeca, Raphael Frank, and Thomas Engel. 2016. Luxembourg SUMO Traffic (LuST) Scenario: 24 hours of mobility for vehicular networking research. *IEEE Vehicular Networking Conference, VNC* 2016-Janua (2016), 1–8.
[4] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, and Jean-Pierre Hubaux. 2007. Mix-Zones for Location Privacy in Vehicular Networks. *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)* 51 (2007), 1–7.
[5] Mohammad Khodaei, Hongyu Jin, and Panos Papadimitratos. 2015. Towards deploying a scalable & robust vehicular identity and credential management infrastructure. *IEEE Vehicular Networking Conference, VNC* 2015-January, January (2015), 33–40.
[6] Mohammad Khodaei, Hongyu Jin, and Panos Papadimitratos. 2018. SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems. *IEEE Transactions on Intelligent Transportation Systems (IEEE ITS)* (April 2018).