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, Sweden
www.ee.kth.se/nss

Security System Entities
• Vehicles registered with one (home) Long Term Certification Authority (LTCA)
• Pseudonym Certification Authority (PCA) servers in one or multiple domains
• Vehicles can obtain pseudonyms from any PCA (in home or foreign domain)
• Trust across domains with the help of a Root CA (RCA) or cross-certification

Security & Privacy Requirements
• Authentication and communication integrity
• Authorization and access control
• Non-repudiation, accountability and eviacion
• Conditional anonymity & unlinkability

Adversarial Model
• Honest-but-curious VPKI entities
• Adversaries could eavesdrop VC systems to infer user-sensitive information, derived from Cooperative Awareness Messages (CAMs), e.g., timing, velocity, heading, and location, to harm user privacy

Pseudonym Acquisition Policy

Vehicular Communication (VC) Systems

Figure 1. Vehicular Public-Key Infrastructure (VPKI) Architecture [7,9].

SECMAVE Overview

Figure 3. Pseudonym Acquisition Overview in Home and Foreign Domains [7,12].

Mitigating Timing-based Inferences

Figure 4. Universally Fixed Policy [7,9,12].

Solution 1: Mix-zones Everywhere

• Upon reaching a pseudonym transition process, a dynamic mix-zone is initiated
• All CAMs within each mix-zone are encrypted using a distinct symmetric session key
• Dynamic formation of mix-zones combined with the fully-unlinkable pseudonym issuance process hinder harming user privacy by colluding entities, e.g., a VPKI entity

Solution 2: A Vehicle-centric & Cooperative Mix-zone Scheme

• Mitigating syntactic & semantic linking attacks
• Requires having vehicles provided with pseudonyms with overlapping lifetimes
• Preventing malicious internal vehicles from degrading the anonymity set
• Strongly protecting user privacy in the presence of honest-but-curious VPKI entities

Remaining Challenges
• Efficient, scalable, and resilient group authentication scheme to initiate dynamic formation of mix-zones
• Evaluating the performance of the two solutions in simulation and gauging the achieved privacy protection

Infering User-sensitive Information
• Syntactically and semantically (i.e., time and velocity) linking messages
• Linking based on times of pseudonym changes (cannot be obfuscated)

Mix-Zone Initiation Protocol

References