COSMO
CONNECTED · SMART · MOBILITY

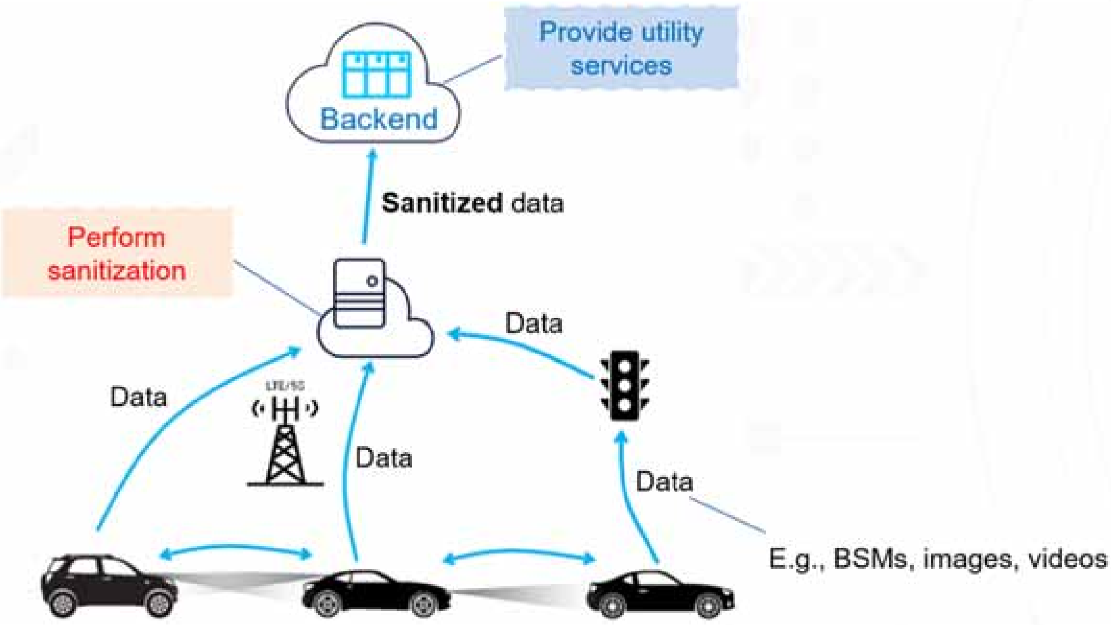
Technology Offer

Privacy-Aware Service Provisioning In V2X Networks

Technology Overview

In a V2X network, agents (including vehicles and pedestrians) are highly dynamic and safety consideration is always of the highest priority. We developed a new privacy framework to deal specifically with V2X networks, leveraging on the C-V2X and DSRC infrastructure. We bring inference privacy mechanisms to ITS networks. Inference privacy refers to the prevention of a service provider from performing statistical inference it has not been authorized to do. Our privacy-preserving framework can be efficiently implemented in vehicle OBUs, RSUs and gNodeBs to achieve monitoring and service provisioning while ensuring inference and data privacy with low computational overhead.

Our framework can be used to sanitize different kinds of C-V2X data such as basic safety message (BSM), images, video clips, etc. in order to suppress the embedded private information while maintaining the information necessary for the service provider to perform authorized tasks.



Technology Features / Specification

The technology consists of a pending patent and software algorithms. The patent is related to a framework for sanitizing various privacy sensitive C-V2X data.

Our privacy-preserving framework is a lightweight deep learning model which takes raw data such as BSMs and images as the inputs and outputs sanitized data with private information in the raw data maximally suppressed while the utility information is minimally distorted. Hence, the users of our technology can submit the privacy-preserved data instead of the raw data to the service provider.

Our framework can be trained offline and implemented in real-time on either portable devices or an edge server.

To deploy our framework, no modification is required in the current V2X communication systems because the size and the shape of the sanitized data are the same as those of the raw data.

Potential Applications

Insurance companies may assess a driver's risk by collecting and analyzing his/her driving data via basic safety messages (BSMs) to determine the premium to be charged for the personal auto insurance. From the BSMs, insurers can recognize their customers' driving patterns, e.g., normal or aggressive. Meanwhile, they are also able to infer other information from BSMs such as the locations their customers have been to. In our solution, we sanitize BSMs to obfuscate location information while maintain quality of utility services, e.g., recognition of {normal, aggressive, drowsy} driving.

In an autonomous people mover, the actions of the passengers are monitored by in-vehicle cameras. When passengers are performing aggressive, dangerous or suspicious actions, an alert should be raised. However, during normal operations, passengers' personal identities are sensitive and private information. As a proof-of-concept, consider the following setup: We sanitize images/video clips captured by in-vehicle camera such that distraction actions such as talking on the phone, texting on the phone, etc., can be correctly recognized while the driver's sensitive information, e.g., gender, race, are maximally removed.

Benefits

The technology restricts the utility of C-V2X data to a service provider's authorized mode of usage while minimizing the risk that the data can be repurposed for other uses, including the tracking of a vehicle.

Please contact A/Prof. Tay Wee Peng (NTU) for further discussions on this technology.

CONNECTED · SMART · MOBILITY
www.ntu.edu.sg/ciss/research-capabilities/research-programmes/cosmo

Connected Smart Mobility Programme
School of Electrical and Electronic Engineering
Nanyang Technological University
50, Nanyang Avenue, S2-B3b-10, Singapore 639798

(65) 6790 5468
cosmo@ntu.edu.sg