63rd FITCE International Congress

26 – 28 September 2024, Kraków, Poland

κ-anonymity in Resource Allocation for Vehicle-to-Everything (V2X) Systems

Andres Vejar, **Faysal Marzuk**, Piotr Chołda

Institute of Telecommunications

AGH University of Krakow, Kraków, Poland

Outline

1. **Introduction**
   - Vehicle-to-Everything (V2X) Systems
   - Privacy-Enhancing Technologies (PET)
2. **System Model**
   - V2X Communication System Model
   - Centralized vs. κ-anonymous Allocation Models
3. **Results and Evaluation**
4. **Conclusion and Future Work**

Introduction

Vehicle-to-Everything (V2X) systems

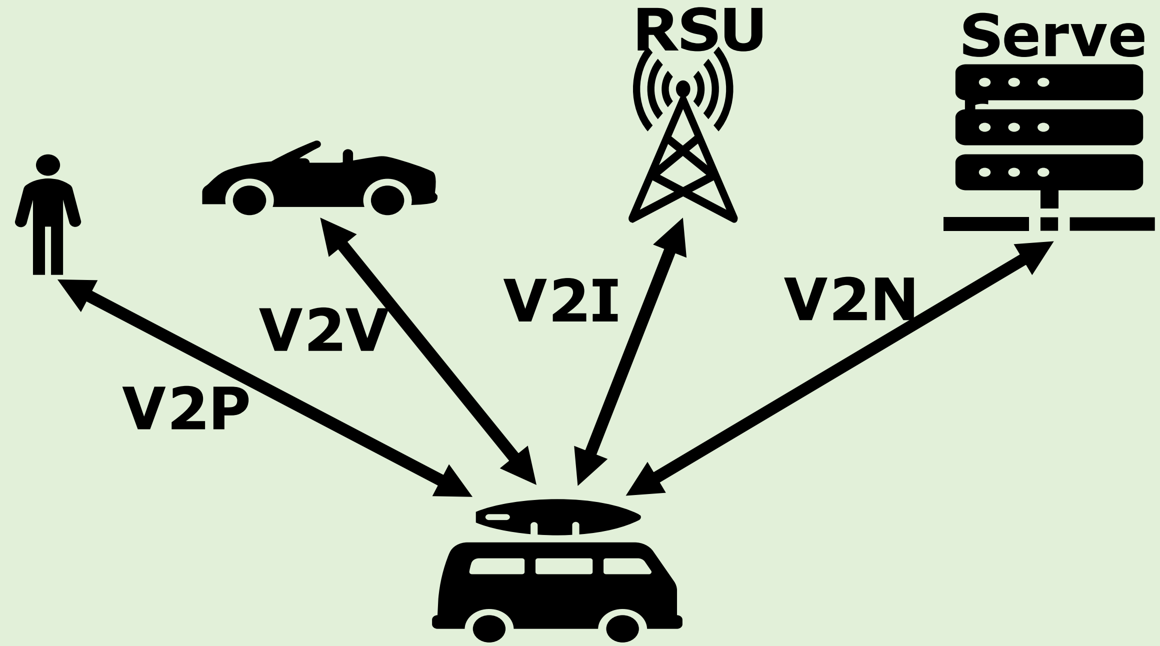

Figure 1: Types of V2X communications.

Introduction

6G V2X vulnerabilities and design challenges

- 6G V2X communication systems are vulnerable to security attacks due to
  - high mobility
  - dynamic topology
  - various communications

- Designing V2X networks that integrate AI technology is challenging because
  - it needs to include robust security mechanisms
  - It needs to consider privacy and ethics

Introduction
6G V2X protection of user privacy

- Built-in privacy to collect and process user data in V2X systems
- Reducing the risk of reidentification and unauthorized monitoring

- In designing secure V2X systems, anonymization techniques are used to
  - protect identity of system’s users
  - reduce specific vehicles’ information

- Privacy-enhancing technologies (PETs) are required, including methods of
  - differential privacy
  - data anonymization

6G V2X privacy on *compromised* resource allocation

- If resource allocation systems are infiltrated by malicious entities, revealing sensitive information such as vehicle locations poses a risk to user privacy
  - **Identification of each vehicle is available to attackers**
  - **Acquired information can be used to escalate attacks to other system's elements**
- It is important to reduce the attack surface in the infrastructure
  - **Zero-trust architectures / privacy by design**
  - **Essential data security and privacy preservation**
- Addressing requirements for 6G V2X allocation process

V2X Communication System

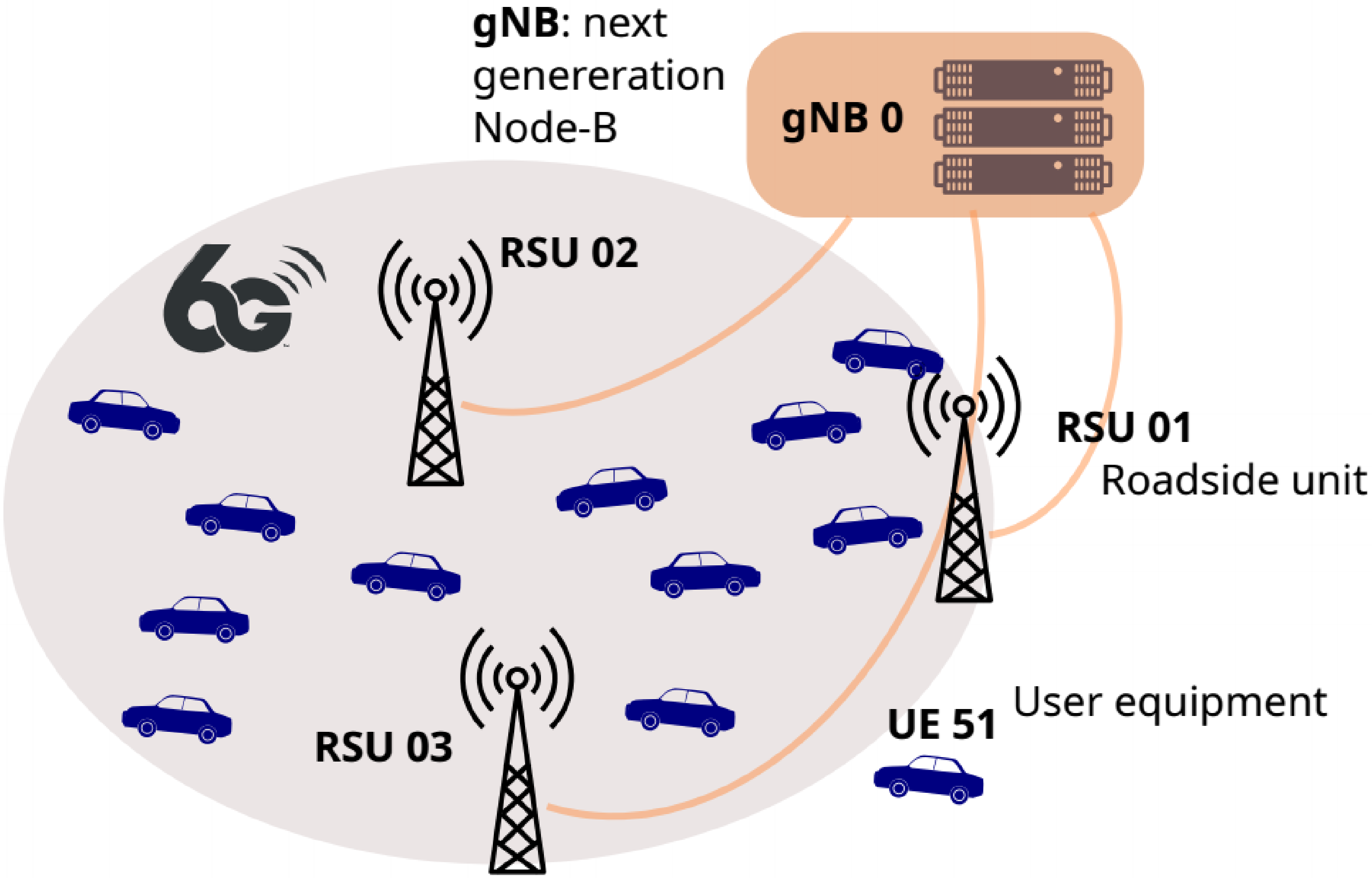

Figure 2: An example of a V2X communication system.

Centralized Allocation System

- A centralized allocation system requires specific information of the participating vehicles
- The vehicles communicates the information to get assigned to one RSU
- The centralized allocation system generate an optimal (or near optimal) assignation for all the participating vehicles
- The vehicles upload tasks to the assigned RSU

To solve the allocation problem in a realistic scenario, the vehicle information includes:

- communication demand: $\boldsymbol{D_v} \in [\mathbf{10} - \mathbf{60}]$ **kbits**
- computation demand: $\boldsymbol{\phi_v} \in [\mathbf{100} - \mathbf{150}]$ **cycles/bit**
- transmission power: $\boldsymbol{P_v} \in [\mathbf{23} - \mathbf{33}]$ **dBm**

Centralized Allocation Privacy Risk

- $(\boldsymbol{D}_v, \boldsymbol{\phi}_v, \boldsymbol{P}_v)$ is used in the centralized allocation to calculate
  - communication and computation delays
  - energy consumption

- If the allocation system is breached, the vehicle information can be exploited to uncover, monitor and further compromise individual vehicles.

- Design V2X systems with privacy enhancing techniques reduce the probability of unauthorized tracking and re-identification.

Results & Evaluation

- V2V communication to achieve k-anonymity through proximity clusters
- Assuming that V2V communication is secured in its radius of operation
- Triplet $(\boldsymbol{D_v}, \boldsymbol{\phi_v}, \boldsymbol{P_v})$ is distributed in vehicle's proximity cluster
- Aggregate measurement is pooled into its average value
- Each vehicle transmits to RSUs aggregated triplet values $< \boldsymbol{D_v}, \boldsymbol{\phi_v}, \boldsymbol{P_v} >$
- gNB estimates $\mathbf{SINR}$ values of each vehicle with respect to each RSU
- $\mathbf{SINR}$ values are aggregated for each proximity cluster $< \mathbf{SINR} >$
- Cluster's membership is verified by vehicles sharing the same $< \boldsymbol{D_v}, \boldsymbol{\phi_v}, \boldsymbol{P_v} >$
- k-private allocation system receives only
  - $< \boldsymbol{D_v}, \boldsymbol{\phi_v}, \boldsymbol{P_v} >$ from vehicles
  - $< \mathbf{SINR} >$ from gNB

Results & Evaluation (cont'd)

- We compare k-anonymous V2X allocation vs. centralized allocation models
- Scenarios with densities of $\mathbf{126\ RSUs/km^2}$ and $\mathbf{1000\ vehicles/km^2}$
- For $\mathbf{190}$ vehicles not all constraints are satisfied
- Reduced energy consumption in k-anonymous version

Allocation	selected/available RSUs	# Vehicles	Energy
Centralized	2/4	32	0.002432
k-anonymous	2/4	32	0.002459
Centralized	4/16	127	0.005532
k-anonymous	5/16	127	0.006830
Centralized	7/24	190	0.009790
k-anonymous	7/24	190	0.008454

Conclusion & Future Work

- k-anonymity for privacy and efficiency requirements in V2X networks
- k-anonymity method used to maintain and preserve location privacy
- Protection against inference and gradient leakage attacks
- Our implementation shows how variations in optimal allocations are affected when PET is applied to V2X systems
- More advanced techniques, considering the incorporation of online allocation by AI models

63rd FITCE International Congress

26 – 28 September 2024, Kraków, Poland

Thank you for your attention!