
Sujash Naskar
Department of Information System and Technology (IST)
Contact: sujash.naskar@miun.se


Sensible Things that Communicate
Prof. Mikael Gidlund
Contact: mikael.gidlund@miun.se

Internet of Vehicles (IoV)-Privacy and Security

Introduction

To make futuristic automated transportation a reality, Vehicular-ad-hoc-Network and IoT are combined to form IoV. To ensure passenger safety in automated vehicles and to have reliable, intelligent transportation of goods, all communications in IoV must be secured with authenticity, key sharing, and encryption-decryption of messages.

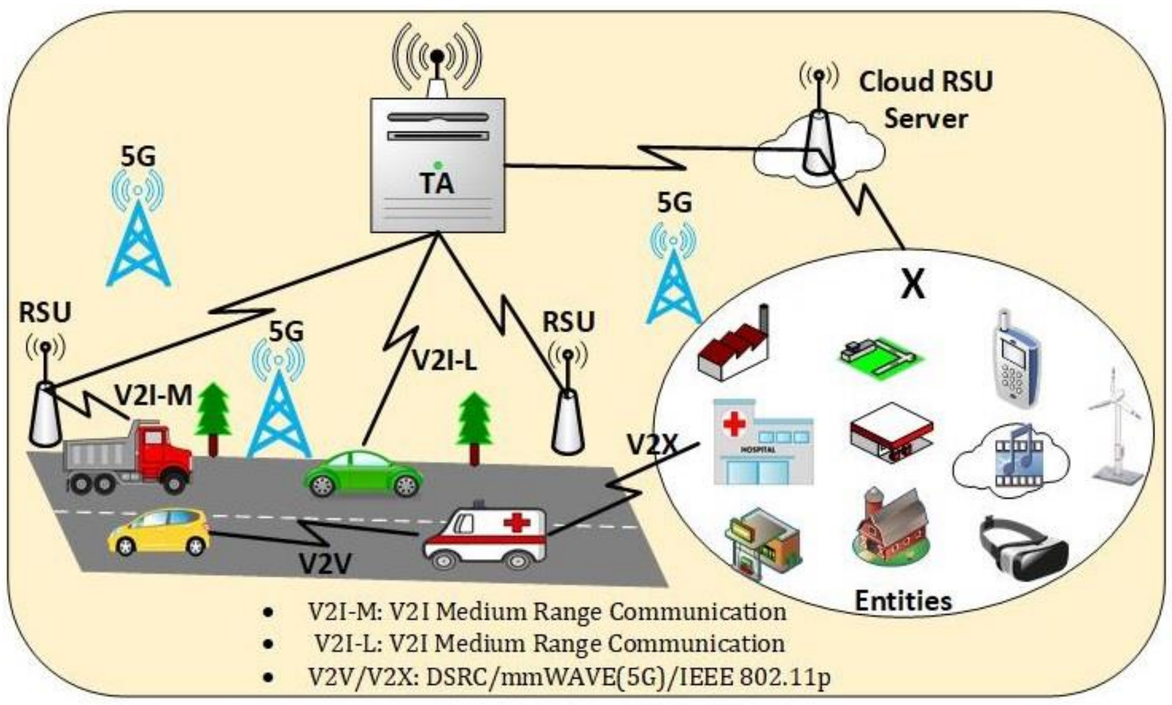


Fig: IoV Architecture

1. Need of IoV

Global Statistic of Traffic Injuries by WHO:

- 1.3 million people die each year
- 20 to 50 million suffer injuries
- 3% of gross domestic product loss
- Globaly 73% of accidents involve men, and in Sweden, this number is 77%

Statistic of Swedish Driving Licence test 2021:

- 59 % of total theory tests failed
- 52% of the total practical tests failed

2. Security Requirement Specification

Vehicle to Authority — Mandatory Authentication ⟷ Public Channel (Internet)

Vehicle to Road Side Unit — Broadcast Key ⟷ Insecure Channel

Vehicle to Vehicle — Symmetric Key Share ⟷ Insecure Channel

Vehicle to Others (X) — Hide Privacy ⟷ Insecure Channel

3. Our Proposed Approach

- Pseudo random value based anonymous privacy-preserving authentication using SHA-256, SHA-384
- Use of quadratic residuocity problem: $x^2 \equiv a\ (mod\ m)$

  Legendary Symbol, $\left(\frac{a}{q}\right) = \begin{matrix} 1\ if\ a\ is\ a\ QR\ modulo\ q \\ -1\ if\ a\ is\ a\ NQR\ modulo\ q \end{matrix}$

  Eulers Criterion: $\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} (mod\ q)$ to share Key.

4. Results

Security Type	Execution Time	Message Size
Authentication	0.032 ms	182 / 116 bytes
Group key (128-bit key)	40ms	288 bytes
Token Share	0.048ms	40 bytes

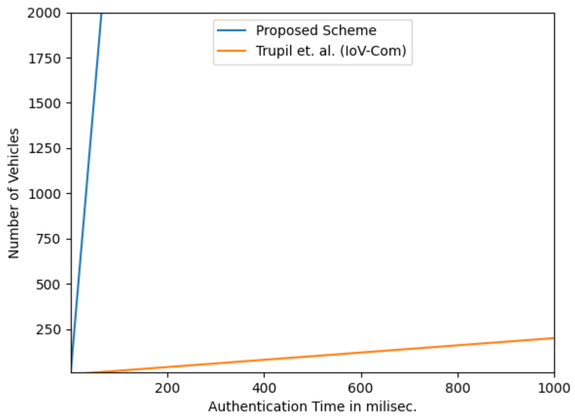
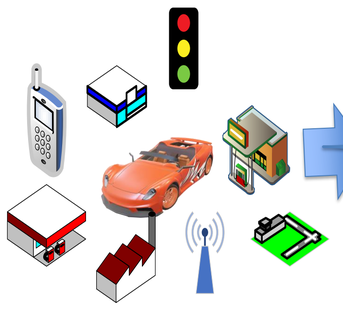


Fig: Verification Time

5. Beneficiaries

We Design and develop Security Protocols → Used by → Car Manufacturers and Traffic Authorities → Implemented and installed → OBU/TPU → IoV- Entities



Benefits: Decrease Road Accidents; Reliable and Efficient goods Transport; Comfortable and Secure Travels → Safe Society