

Anonymous Key Agreements for V2X Communication

Gautam Singh

Indian Institute of Technology Hyderabad

May 1, 2024

1 Introduction

2 Preliminaries

3 Our Proposition

4 Conclusion

V2X Related Terminology

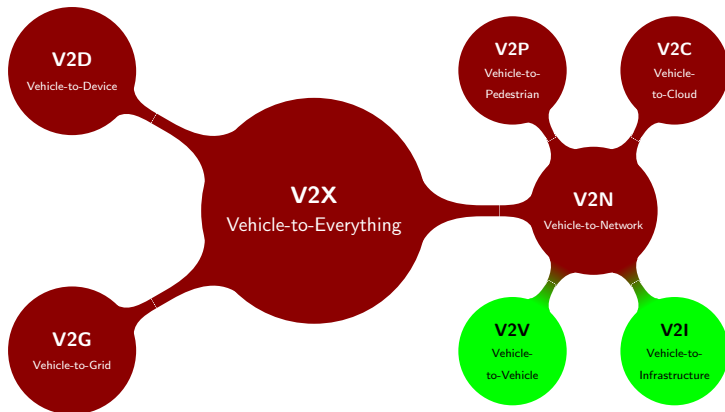


Figure 1: A breakdown of V2X.

Message Types in V2X

① **Cooperative Awareness Messages (CAMs)**¹ and **Basic Safety Messages (BSMs)**².

- 1 Exchanged between vehicles to create awareness and support cooperative performance of vehicles in the road network.
- 2 Includes status information such as time, position, speed, active systems, vehicle dimensions, etc.
- 3 Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
- 4 **Huge privacy concerns and threats!**

¹European Telecommunications Standards Institute. "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service". In: ETSI EN 302 637-2 V1.4.1 (2019). URL: https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.04.01_60/en_30263702v010401p.pdf.

²J2735_202309: V2X Communications Message Set Dictionary - SAE International. URL: https://www.sae.org/standards/content/j2735_202309/ (visited on 04/15/2024).

Message Types in V2X

① **Cooperative Awareness Messages (CAMs)¹ and Basic Safety Messages (BSMs)².**

- ① Exchanged between vehicles to create awareness and support cooperative performance of vehicles in the road network.
- ② Includes status information such as time, position, speed, active systems, vehicle dimensions, etc.
- ③ Broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
- ④ **Huge privacy concerns and threats!**

② Other types of messages

- ① **Signal Phase and Timing (SPaT)**
- ② **Roadside Infrastructure Information (MAP)**

¹European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

²J2735_202309.

Motivation and Goals

- ① Do we *really* need to encrypt CAMs?
 - Google (Maps) may already be profiling us!
 - Focus on encrypting more sensitive messages and information sent less frequently.

Motivation and Goals

- ① Do we *really* need to encrypt CAMs?
 - Google (Maps) may already be profiling us!
 - Focus on encrypting more sensitive messages and information sent less frequently.
- ② Unlimited privacy.

Motivation and Goals

- ① Do we *really* need to encrypt CAMs?
 - Google (Maps) may already be profiling us!
 - Focus on encrypting more sensitive messages and information sent less frequently.
- ② Unlimited privacy.
- ③ Negligible storage and bandwidth overheads.

Motivation and Goals

- ① Do we *really* need to encrypt CAMs?
 - Google (Maps) may already be profiling us!
 - Focus on encrypting more sensitive messages and information sent less frequently.
- ② Unlimited privacy.
- ③ Negligible storage and bandwidth overheads.
- ④ Better security guarantees (privacy, authenticity, confidentiality).

Pairings

Anonymous Key Agreements

Proposed Security Flow

Analysis

Conclusion and Future Works