Anonymous Key Agreements for V2X Communication

Gautam Singh

Indian Institute of Technology Hyderabad

May 1, 2024

V2X Related Terminology

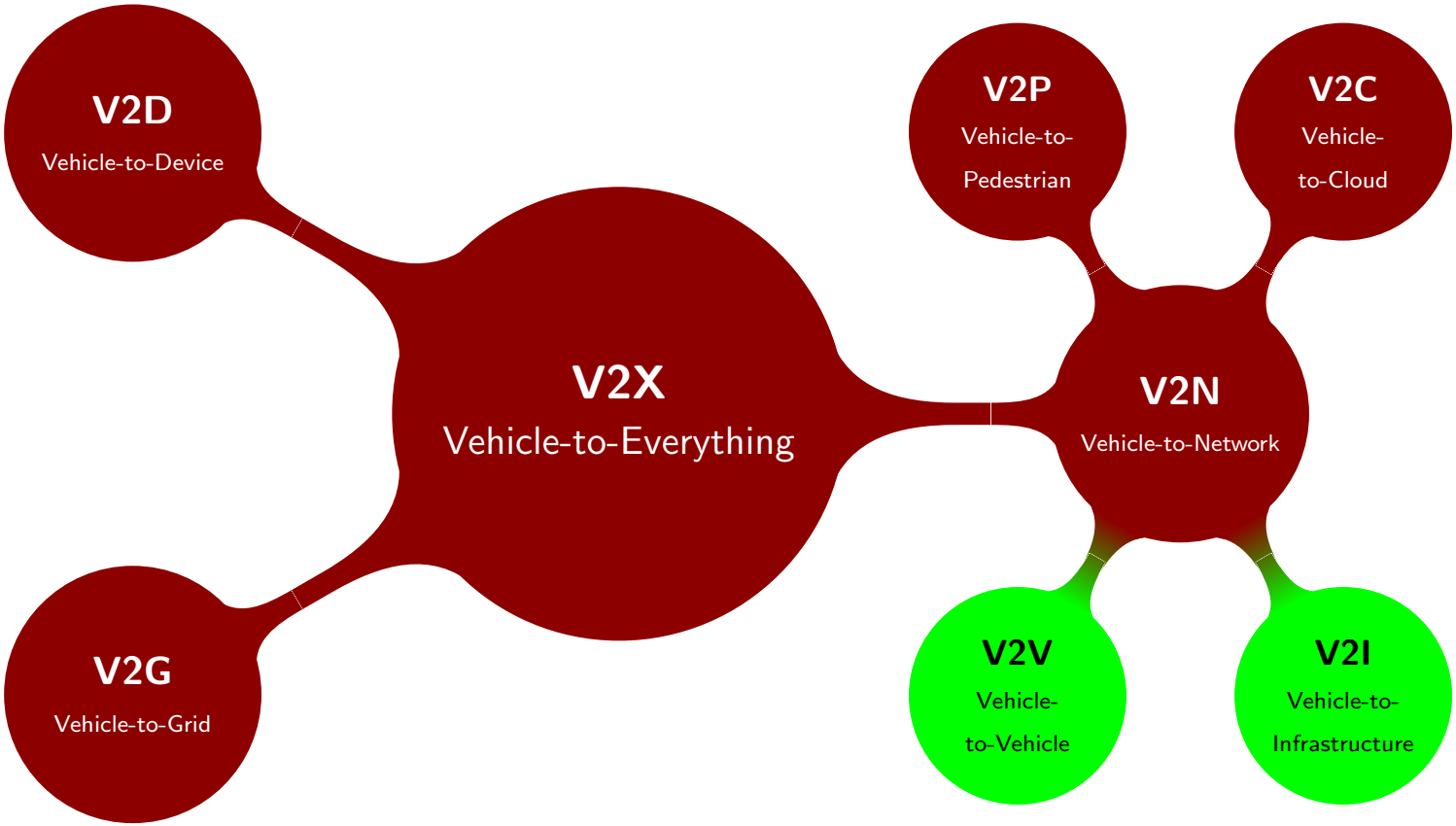

Figure 1: A breakdown of V2X.

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!**

[1] European 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.

[2] *J2735_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)

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

[2] *J2735_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

Definition 1

Pairing Let $\mathbb{G}_0 = \langle g_0 \rangle$, $\mathbb{G}_1 = \langle g_1 \rangle$, $\mathbb{G}_T$ be three cyclic groups of prime order q. A *pairing* is an efficiently computable function $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$ satisfying the following properties:

1. *bilinear*: for all $u, u' \in \mathbb{G}_0$ and $v, v' \in \mathbb{G}_1$, we have

$$e\left(uu', v\right) = e\left(u, v\right) e\left(u', v\right) \tag{1}$$
$$e\left(u, vv'\right) = e\left(u, v\right) e\left(u, v'\right) \tag{2}$$

2. *non-degenerate*: $g_T := e\left(g_0, g_1\right)$ is a generator of $\mathbb{G}_T$.

1. Here, $\mathbb{G}_0$ and $\mathbb{G}_1$ are called *source groups* and $\mathbb{G}_T$ is called the *target group*.
2. When $\mathbb{G}_0 = \mathbb{G}_1$, the pairing is said to be *symmetric*.

Anonymous Key Agreement

1. A key agreement protocol where two parties agree on a shared secret key, without being able to determine the other party.

Anonymous Key Agreement

1. A key agreement protocol where two parties agree on a shared secret key, without being able to determine the other party.
2. Pairing-based anonymous key agreement for V2X
   - Clients should authenticate each other.
   - Clients should not be able to determine the identity of each other.

Attributes, Credentials, Anonymous Credentials

1. **Attributes**: Labels associated with a user that describe them fully, such as role of a user.

Attributes, Credentials, Anonymous Credentials

1. **Attributes**: Labels associated with a user that describe them fully, such as role of a user.
2. **Credential**: Data possessed by a user that demonstrates their attributes.

Attributes, Credentials, Anonymous Credentials

1. **Attributes**: Labels associated with a user that describe them fully, such as role of a user.
2. **Credential**: Data possessed by a user that demonstrates their attributes.
3. **Anonymous Credential**: Data possessed by a user that demonstrates their attributes, *without revealing any additional information* about their identity.

Attributes, Credentials, Anonymous Credentials

1. **Attributes**: Labels associated with a user that describe them fully, such as role of a user.
2. **Credential**: Data possessed by a user that demonstrates their attributes.
3. **Anonymous Credential**: Data possessed by a user that demonstrates their attributes, *without revealing any additional information* about their identity.
4. For V2X, we require anonymous credentials to be issued to vehicles regularly to ensure anonymity as well as to check legitimacy of that vehicle.

Proposed Message Flow

Analysis

Conclusion and Future Works