Zone Encryption with Anonymous Authentication for V2V Communication

Jan Camenisch, Manu Drijvers, Anja Lehmann, Gregory Neven and Patrick Towa

Gautam Singh

Indian Institute of Technology Hyderabad

April 23, 2024

V2X Related Terminology

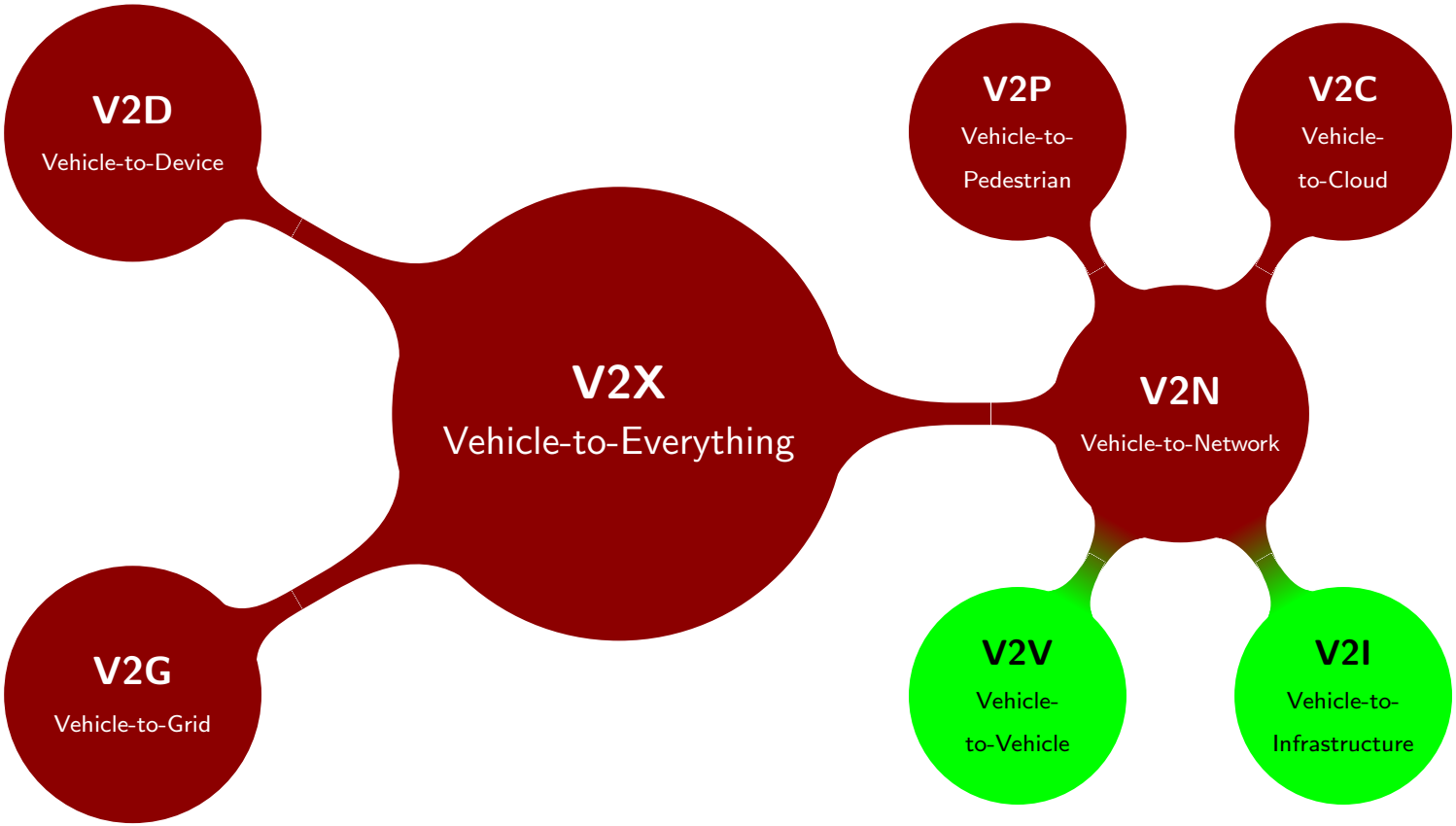

Figure 1: A breakdown of V2X.

Message Types in V2X

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

Message Types in V2X

1. **Cooperative Awareness Messages** (CAMs) [1] and **Basic Safety Messages** (BSMs)
   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.
2. Other types of messages
   1. **Signal Phase and Timing** (SPaT)
   2. **Roadside Infrastructure Information** (MAP)

V2X and Cryptology

1. CAMs broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
    1. Frequently broadcast: 1 CAM per second in US, 10 per second in EU.
    2. Easy to intercept.
    3. Leak sensitive information about the vehicle owners.

V2X and Cryptology

1. CAMs broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
   1. Frequently broadcast: 1 CAM per second in US, 10 per second in EU.
   2. Easy to intercept.
   3. Leak sensitive information about the vehicle owners.
   4. **Huge privacy concerns and threats!**

V2X and Cryptology

1. CAMs broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
   1. Frequently broadcast: 1 CAM per second in US, 10 per second in EU.
   2. Easy to intercept.
   3. Leak sensitive information about the vehicle owners.
   4. **Huge privacy concerns and threats!**
2. Encryption impractical, since CAMs *must* be decrypted by nearby vehicles in a highly dynamic environment.
   1. But CAMs *have to* be encrypted because of the data they carry!

V2X and Cryptology

1. CAMs broadcasted unencrypted in 5.9 GHz channel (ETSI ITS-G5).
   1. Frequently broadcast: 1 CAM per second in US, 10 per second in EU.
   2. Easy to intercept.
   3. Leak sensitive information about the vehicle owners.
   4. **Huge privacy concerns and threats!**
2. Encryption impractical, since CAMs *must* be decrypted by nearby vehicles in a highly dynamic environment.
   1. But CAMs *have to* be encrypted because of the data they carry!
3. Instead, focus on *privacy-preserving authentication*.
   1. Ensuring a message is issued by a "genuine" vehicle.
   2. "Genuine" vehicles must be untraceable.

V2X and Cryptology

1. Deployed systems
    1. Use short-term **pseudonym certificates** (100 per week in EU, 20 per week in US), rotate between them.
    2. Trade-off between security (Sybil resistance), privacy and efficiency (storage and bandwidth costs).

V2X and Cryptology

1. Deployed systems
   1. Use short-term **pseudonym certificates** (100 per week in EU, 20 per week in US), rotate between them.
   2. Trade-off between security (Sybil resistance), privacy and efficiency (storage and bandwidth costs).
2. Proposed systems
   1. Stronger privacy and security guarantees.
   2. Do not fit the *stringent bandwidth constraint* of **300 bytes per CAM**, thus they are impractical.

Motivation and Goals

1. Aim to tackle the problem of privacy.
2. Address the problem of authenticity and confidentiality in combination *for the first time* (important to mention this?).
3. Meet (bandwidth) requirements.
4. Efficient encryption scheme (symmetric-key crypto).
5. Better security guarantees (privacy, authenticity, confidentiality).

Preliminaries

This is a slide with the list of preliminaries needed to understand ZE. We pick up the ones not covered (top down approach, start from ZE and then explain these if needed). Must list purpose of each preliminary here.

1. Pairing Groups
2. Hardness Assumptions (lot of notation, may be hard to grasp)
    1. SDL
    2. q-MSDH-1
3. Deterministic Authenticated Encryption (how much to cover?)
4. PS Signatures
5. DGS+A

Syntax of ZE Scheme

1. Define zone, payload, epoch.
2. Explain all the algos used.

Security Properties

Attack game and definitions 3-6 (are theorems 4-8 needed?)

Instantiation of ZE and Efficiency

(Is it worth mentioning section 4.4.1 or can we leave this?)

Summary of ZE

Table 2 of the paper.

DGS+A

Sub-headings

1. Syntax
2. Security properties (no proofs)
3. Instantiation from PS
4. Can be extended to threshold opening (should be a slide or only a mention during talk?)

Challenges in Deploying ZE

Section 4.6

Future Improvements

Section 4.6, brief and top-level idea of mini-project if time permits.

References I


European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," no. ETSI EN 302 637-2 V1.4.1, 2019.