Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

Future generation Security for smart and connected Cars - FuSeCar

Deliverable D1.1: Methodology for de-anonymization and linkability in realistic connected vehicle scenarios

WP1: Privacy analysis of current vehicular communications protocols and architectures

Authors:
Giovanni Gambigliani Zoccoli[1], Mirco Marchetti[1], Mauro Andreolini[2], Luca Ferretti[2], and Mattia Trabucco[2]
{name.surname}@unimore.it

[1]Department of Engineering "Enzo Ferrari"
[2]Department of Physics, Informatics and Mathematics
University of Modena and Reggio Emilia

Current revision: R1.2
Delivery date: December 22th, 2023

Revision history

Authors	Changes	Date	Revision
Giovanni Gambigliani Zoccoli, Mirco Marchetti	Creation of the document, tentative structure	September 2nd, 2024	R0.1
Giovanni Gambigliani Zoccoli, Mirco Marchetti	First draft of Section 2	September 9th, 2024	R0.2
Mauro Andreolini, Giovanni Gambigliani Zoccoli	First draft of Section 3	September 19th, 2024	R0.3
Mirco Marchetti, Giovanni Gambigliani Zoccoli, Luca Ferretti	First draft of complete document	October 28th, 2024	R1.0
Mirco Marchetti, Giovanni Gambigliani Zoccoli, Luca Ferretti, Mauro Andreolini	Updates of draft based on WP1 results, Minor fixes	November 7th, 2024	R1.1
Mattia Trabucco, Giovanni Gambigliani Zoccoli	Updated document with new template, minor fixes	December 1st, 2025	R1.2

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

Contents

1 Introduction

This deliverable is a technical report including the result of Work Package WP1: Privacy analysis of current vehicular communications protocols and architectures. This WP includes preliminary study activities that are required for the following steps of the project, and has two main outcomes: the first is highlighting how the current privacy preserving solutions deployed in VANETs network are unable to effectively anonymize drivers. the second is to describe how an attacker in possession of simple hardware and software equipment is able to monitor the communications issued by the vehicles and track vehicle's movements.

1.1 Introduction to VANETs and C-ITS

Vehicular Ad Hoc Networks (VANETs) are a subclass of Mobile Ad Hoc Networks (MANETs) specifically designed to enable communications between vehicles and infrastructure. These networks play a crucial role in Cooperative Intelligent Transport Systems (C-ITS), which aim to enhance traffic efficiency, safety, and environmental sustainability by facilitating real-time data exchange.

VANETs primarily involve two types of communication:

- Vehicle-to-Vehicle (V2V) Communication: Vehicles exchange safety and traffic-related messages, such as collision warnings, lane change notifications, and emergency braking alerts.
- Vehicle-to-Infrastructure (V2I) Communication: Vehicles interact with roadside units (RSUs) and other infrastructure to receive updates on road conditions, traffic lights, and other transport information.

These communications rely on wireless technologies, particularly IEEE 802.11p (DSRC) and Cellular-V2X (C-V2X), to ensure low-latency and high-reliability message exchange. However, while these technologies enhance road safety and efficiency, they also introduce serious privacy risks, as vehicles continuously broadcast messages that could be intercepted and analyzed by adversaries.

1.2 Other communication protocols available on vehicles

In addition to VANET-specific communication protocols, modern vehicles are equipped with multiple wireless communication technologies that facilitate connectivity and functionality:

- Wi-Fi (IEEE 802.11): Vehicles are equipped with Wi-Fi modules for internet access, software updates, infotainment systems, and hotspot functionality. These Wi-Fi signals contain unique MAC addresses [1] and other fields that can be used to track the vehicles. Despite the IEEE 802.11 standard not specifying the probing interval required to send these messages (with a de-facto default configuration of 100 ms, the maximum transmission power is set equal to 20 dBm, equivalent to 100 mW).
- Bluetooth: Used for hands-free calling, wireless audio, and connectivity with mobile devices and wearable technology. Bluetooth communications also include unique identifiers in the header, such as device MAC addresses, making them useful for tracking. To discover new devices with the Bluetooth protocol the standard imposes the advertising mechanism which consists of broadcasting information to make themselves discoverable without establishing a connection. Since the Bluetooth protocol is used for short range data exchange the maximum transmission power is set to 20 dBm, but depending on the application this value can be reduced. Moreover, since Bluetooth is designed to keep energy consumption as low as possible the advertising interval is variable starting from 20 ms up to 10 seconds [4].
- Tire Pressure Monitoring System (TPMS): Wireless sensors transmit tire pressure data to the vehicle's onboard system. TPMS communications contain unique identifiers, which can be leveraged to track a specific vehicle using predefined frequencies: 315MHz and 433MHz.

The presence of unique identifiers in the payload or header of these protocols presents a significant privacy risk, as attackers can exploit these signals to track vehicles, correlating them with messages sent in the VANET.

The privacy preserving techniques deployed in the VANETs network and their limitations are described in Section 2. The thread model presenting how a realistic attacker equipped with simple antennas is described in Section 3. The attack methodology which describes how the attacker is capable to link the pseudonyms and track the vehicle inside the scenario is presented in Section 4. The conclusion is reported in Section 5.

2 Privacy preserving techniques in VANETs

Vehicular networks continuously broadcast messages containing crucial information such as vehicle position, speed, and safety alerts. One of the biggest concerns in VANETs is the potential for vehicle tracking and driver de-anonymization. As vehicles continuously exchange messages, an adversary could monitor these transmissions to identify and track a vehicle over time. To mitigate these risks, pseudonym-based schemes have been implemented under DSRC (Dedicated Short-Range Communications) and ETSI ITS-G5 standards, designed to obscure the real identity of vehicles and prevent tracking. Pseudonymization in VANETs follows an approach in which each vehicle is issued with multiple short-term certificates. These certificates are periodically changed to make it difficult for an observer to correlate different messages to the same vehicle. Vehicles are preloaded with a set of digital certificates issued by a trusted Certificate Authority (CA). Each certificate corresponds to a temporary identity (pseudonym) used in VANET messages. To enhance privacy, vehicles periodically switch to a new pseudonym, discarding the previous one depending on different strategies (pseudonyms change scheme) which are usually based on time, frequency, vehicle density and vehicle collaboration, however remaining an open project [2, 3].

2.1 Weaknesses of Pseudonymization in VANETs

Despite their intended purpose, pseudonym-based privacy solutions are not sufficient to ensure the privacy of the communications in VANETs. If pseudonyms are changed at regular time intervals, an attacker can anticipate when a vehicle's identity is about to switch and correlate subsequent messages to the same vehicle. Another approach is the event-based pseudonym changes which reduce this risk but remain susceptible to timing analysis. In DSRC-based systems, each vehicle changes pseudonyms independently, allowing attackers to isolate individual vehicles in a traffic stream by monitoring vehicles that change pseudonyms while others do not. Without synchronized group changes, attackers can use differential analysis to follow a vehicle's movement despite identity switches. Even if a vehicle's pseudonym changes, other protocols such as Wi-Fi, Bluetooth or TPMS transmissions continue using persistent unique identifiers. An attacker monitoring both VANETs and other onboard communications can correlate pseudonym changes with static identifiers, effectively de-anonymizing the vehicle.

3 Threat Model

In this threat model, we consider a passive attacker who does not inject or alter messages but monitors, collects, and analyzes wireless transmissions from different communication technologies used in modern vehicles. Despite using relatively low-cost, commercially available equipment, the attacker can track vehicles over time, correlate different wireless signals, and de-anonymize vehicles despite the use of pseudonyms.

The attacker aims to:

1. Monitor and capture V2V and V2I messages exchanged within a specific geographic area.
2. Collect and analyze other onboard communications (Wi-Fi, Bluetooth, TPMS) that contain unique identifiers.
3. Identify pseudonym changes in VANETs and attempt to correlate them to track vehicles.
4. Combine multiple data sources to improve tracking accuracy.
5. Bypass pseudonym-based privacy mechanisms by leveraging additional side-channel data.

3.1 Real scenario equipment

The attacker can achieve these goals using low-cost, off-the-shelf hardware widely available in the market. The key components include:

1. Software-Defined Radios (SDRs): Devices such as HackRF One, RTL-SDR, or USRP can be used to capture VANET messages (DSRC or C-V2X) and TPMS signals allowing the attacker to eavesdrop on unencrypted wireless transmissions from vehicles over a wide range of frequencies.
2. Wi-Fi Sniffers: Tools like Kismet or Wireshark can capture Wi-Fi probe requests and data packets broadcasted by many modern vehicles to support infotainment and hotspot functionality. MAC addresses of Wi-Fi signals can serve as persistent identifiers, allowing attackers to track a vehicle even when pseudonyms change.
3. Bluetooth Sniffers: Bluetooth devices constantly broadcast signals to enable pairing processes between devices. Bluetooth Low Energy (BLE) devices, such as mobile phones and infotainment systems, emit advertisements that contain static or semi-static unique identifiers.
4. Multi-Antenna Setup: The attacker deploys multiple antennas in strategic locations, such as Intersections (where vehicles slow down and are easier to capture), or Highway entry/exit ramps (to observe long-term movement patterns).
5. Low-Cost Computing Device for Data Processing: A Raspberry Pi or a small Linux-based PC can store collected data and run correlation algorithms.

We can summarize the data collected, and the equipment used by the attacker with the following table.

Protocols	**Purpose**	**Collected data**	**Equipment used**
DSRC/C-V2X (VANETs)	V2V/V2I safety messaging	CAMs, BSMs, pseudonyms, timestamps	Software-Defined Radios (SDR)
Wi-Fi (802.11x)	Infotainment, software updates	MAC addresses, probe requests	Wireshark or similar
Bluetooth	Hands-free calling, device connectivity	Device names, MAC addresses	Bluetooth dongles
Tire Pressure Monitoring System	Tire pressure monitoring	Unique sensor IDs, timestamps	Simple antenna

Table 1: Attacker's collected data and equipment

Table 1 shows the protocols in the first column and how the protocol is used in the VANETs domain, then the data collected from the attacker and the possible hardware used by the attacker to monitor the communications.

4 Attack methodologies

The pseudonym change mechanism in VANETs is designed to prevent long-term tracking by frequently updating the pseudonyms used to sign the messages broadcasted over the network by the vehicles. However, an attacker capable of monitoring and collecting the messages of the VANETs networks is able to track vehicles inside the scenario.

In this section we propose two different attack methodologies, the first methodology describe a simple attacker capable of monitoring only the DSRC communications therefore the BMSs messages exchanged by the vehicles (Section 4.1), the second approach instead consider an advanced attacker which is able to again monitor the DSRC communications and also monitor and collect other communication protocols described in Section 1.2.

4.1 First methodology (DSRC attacker)

The first methodology considers an attacker capable of monitoring and collecting only the messages of the VANETs network able to track vehicles within the area of coverage of all the antennas. In our tracking process, the attacker tries to associate the last message observed with a particular pseudonym value with a group of plausible messages exhibiting a new pseudonym (i.e. a list of pseudonyms whose value has never been observed before). This association is time-based using the formula:

$$T_{last} < T \leq T_{last} + B_{time} + \Delta tol$$

where T_{last} is the timestamp associated with the last message with our target pseudonym, B_{time} is the time interval between consecutive BSMs sent by the same vehicle (it is the inverse of the sending frequency of 10Hz), while Δtol represents a tolerance of the time interval. The result of this association process is a set of BSMs (each one with a different pseudonym value) that are defined from our algorithm as plausible new pseudonyms associated with our target. To select the most similar vehicle having a new pseudonym value we consider the nearest vehicle (in terms of GPS position), having a similar heading (considering a validity range of $[-45°, +45°]$ from the original heading). Then the candidates BSMs are then sorted in ascending distance order, calculated by applying the Euclidean distance between the message with the old pseudonym and the ones with the new values. The best match is selected as the BSM having a Euclidean distance from the original BSM in proximity (with 2 meters tolerance) to the value obtained by multiplying the timestamp difference between the original message and the candidate one (Δts) for the speed of the original BSM (speed).

4.2 Second methodology (Multi radio signal attacker)

The second methodology instead considers a more sophisticated attacker which is able to monitor and collect multiple radio signals from the VANETs network. By combining multiple radio protocols signals including ones with unique identifiers (such as, Wi-Fi, Bluetooth and TPMS) the attacker is able to track the vehicle's movements between the coverage area of different antennas. In our attack methodology, we focus exclusively on DSRC messages (Basic Safety Messages - BSMs) and Wi-Fi beacon probing messages, excluding Bluetooth and TPMS signals. This choice is driven by both technical and practical considerations. DSRC messages are the primary communication method in VANETs, containing critical vehicular state information such as position, speed, and heading, making them the most relevant data source for tracking and pseudonym linking. Wi-Fi beacons, on the other hand, serve as a persistent identifier emitted by many modern vehicles, allowing correlation across pseudonym changes. While Bluetooth and TPMS signals also provide unique identifiers, they are often transmitted at lower power levels and higher frequency, resulting in smaller communication ranges. As a result, limiting our attack methodology to DSRC and Wi-Fi messages ensures a more feasible, high-impact

analysis while reflecting the most realistic tracking scenario. For tracking vehicle's pseudonyms, we employ the same strategy presented in the attack methodology of Section 4.1. However, we remark that the simple attack methodology is extremely ineffective in tracking the same vehicle over different coverage areas. Hence, to overcome this limitation, we use the Wi-Fi probe message as an additional source of information that allows to associate the different pseudonyms to a single ID that can be used to track the vehicle across different coverage areas. In particular, we design three different metrics to associate a single Wi-Fi ID to the list of pseudonyms belonging to the same vehicle:

- Count: considers the number of beacons received between the DSRC and the Wi-Fi probe;
- Statistical RSSI: considers a simple analysis of the signal's strength of DSRC and Wi-Fi messages;
- Pearson RSSI: considers a more complex analysis of the signal's strength of DSRC and Wi-Fi messages.

The attack can be divided in three different phases. In the first phase, we employ the same strategy presented in Section 4.1 to identify all the different pseudonyms of the same vehicle inside the different coverage areas. In the second phase, we define the list of candidates Wi-Fi IDs by selecting all the IDs that are received by the antenna in the same time period of the pseudonyms associated to the same vehicle. Then, a single Wi-Fi ID is selected based on the heuristics described above. Finally, in the third phase, we use the Wi-Fi ID to reconstruct the trip of the vehicles, extending the capabilities of the attacker to track vehicles beyond the single coverage area.

4.3 Count metric

The Count metric considers only the number of messages collected by the attacker for selecting the best Wi-Fi ID. This metric considers the number of DSRC messages composing the list of pseudonyms associated with the same vehicle and the number of beacons of the Wi-Fi with the same ID. This metric assumes that vehicles do not change the probing frequency during operation.

4.4 Statistical RSSI

The Statistical RSSI metric uses the signal's strength of the different messages (DSRC and Wi-Fi beacons) for the correlation of the pseudonyms and an unique Wi-Fi ID. The selection of the best Wi-Fi probe ID is based on the weighted average of the differences between 7 statistical indexes evaluated over the RSSI of the DSRC messages and Wi-Fi beacons. The selection of the Wi-Fi probe ID is based on the minimum value of the average differences (i.e., the most similar RSSI to the reference DSRC's values) with different weights associated for every index. The list of indexes and their corresponding weights is presented in the following:

- mean RSSI (value): 0.1
- standard deviation RSSI (value): 0.3
- median RSSI (value): 0.1
- max RSSI (value): 0.05
- min RSSI (value): 0.05
- max RSSI (timestamp): 0.2
- min RSSI (timestamp): 0.2

4.5 Pearson RSSI

The Pearson RSSI metric uses a more sophisticated approach based on the Pearson correlation [5] for the selection of the Wi-Fi ID corresponding to the reference pseudonyms. In particular, we used the correlation between the pure RSSI values collected for the DSRC messages and the Wi-Fi beacon and we associate a list of pseudonyms with the Wi-Fi ID that exhibits the highest value of Pearson coefficient.

5 Conclusions

This effective attacker model demonstrates that pseudonym changes alone are insufficient to protect vehicle privacy. Even if vehicles follow strict pseudonym rotation policies, wireless signals from other communication protocols leak unique identifiers, allowing attackers to re-identify vehicles and track them despite pseudonym changes.

By strategically placing antennas in key locations, an attacker can capture and analyze V2V and V2I messages, identifying the moments when a vehicle changes its pseudonym. Moreover, pseudonym changes become ineffective when correlated with persistent identifiers from Wi-Fi, Bluetooth, and TPMS signals, which are continuously broadcast by the vehicle. The ability to link subsequent pseudonyms using simple physics laws, combined with the cross-referencing of external identifiers, allows the attacker to effectively reconstruct vehicle trajectories over time. This means that even vehicles implementing standardized privacy-preserving mechanisms remain vulnerable to long-term tracking and de-anonymization attacks.

References

[1] IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, 2021.

[2] ETSI TS 102 941 V2.2.1. Intelligent Transport Systems (ITS); Security; Trust and Privacy Management, 2021.

[3] Matthias Gerlach and Felix Guttler. Privacy in vanets using changing pseudonyms - ideal and real. In *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, 2007.

[4] Bluetooth Special Interest Group. Core specification 6.0, 2024.

[5] Philip Sedgwick. Pearson's correlation coefficient. *BMJ*, 2012.