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 D1.2: Results on de-anonymization and linkability simulations

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: February 29th, 2024

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

Contents

1 Introduction **4**

2 Simulation setup **5**
- 2.1 OMNeT++ (Objective Modular Network Testbed in C++) [5] 5
- 2.2 SUMO (Simulation of Urban Mobility) [3] 5
- 2.3 Veins (Vehicles in Network Simulation) [1] 5
- 2.4 F^2MD (Framework for Misbehavior Detection) [2] 5

3 Scenario **7**
- 3.1 MASA (Modena Automotive Smart Area) [4] Scenario: 7
- 3.2 Pisa Scenario: 7
- 3.3 Catania Scenario: 7

4 Performance evaluation **8**
- 4.1 DSRC attacker 8
- 4.2 Multi radio signal attacker 8

5 Conclusions **11**

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 one main outcome:

- describe the simulations setup used to perform the simulations and present the results obtained with both attack methodologies described in the Deliverable D1.1 titled: Methodology for de-anonymization and linkability in realistic connected vehicle scenarios

The simulation environment and the analysis of the tools used to simulate a realistic scenario to evaluate the linking performance of the tracker is presented in Section 2. Section 3 presents the three different scenarios used in the simulation: Modena, Pisa and Catania. The performance evaluation is described in Section 4 while the conclusions are reported in Section 5.

2 Simulation setup

To analyze the effectiveness of pseudonym change schemes and assess the feasibility of de-anonymization attacks in VANETs, we established a realistic simulation environment using OMNeT++, Veins, and SUMO. This setup enables the modeling of vehicle mobility, V2V/V2I communications, and attacker behavior in a controlled yet realistic environment.

2.1 OMNeT++ (Objective Modular Network Testbed in C++) [5]

OMNeT++ is a powerful, modular, discrete-event network simulator primarily used to simulate complex communication systems and protocols. OMNeT++ supports highly customizable and extensible network models through a flexible module-based architecture. It allows researchers to define various network layers, including physical, MAC, network, and application layers, facilitating detailed analysis of communication performance and security. OMNeT++ is known for its scalability and accurate timing precision, making it suitable for simulating the real-time message exchange required in vehicular communications.

2.2 SUMO (Simulation of Urban Mobility) [3]

SUMO is an open-source, microscopic traffic simulation tool widely used to accurately model the movements and behaviors of individual vehicles within road networks. SUMO enables the detailed definition of traffic scenarios by incorporating realistic parameters such as vehicle speed, acceleration, deceleration, route selection, and driver behavior. By simulating individual vehicle trajectories, SUMO provides precise mobility data, which is essential for understanding how vehicles move through urban or highway scenarios.

2.3 Veins (Vehicles in Network Simulation) [1]

Veins acts as a bridge between SUMO and OMNeT++, integrating detailed traffic simulations with realistic network communication modeling. Veins couples the accurate mobility modeling provided by SUMO with OMNeT++'s extensive capabilities in simulating wireless communications. It implements standard vehicular communication protocols, notably IEEE 802.11p (DSRC) and ETSI ITS-G5, and facilitates realistic V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) interactions. Veins also includes capabilities for simulating message broadcasting, interference, propagation effects, and reception, making it ideal for evaluating vehicular network protocols and privacy schemes under realistic conditions.

2.4 F^{2}MD (Framework for Misbehavior Detection) [2]

The Framework for Misbehavior Detection (F2MD) is a simulation environment designed to evaluate misbehavior detection algorithms within vehicular networks. While F2MD primarily focuses on identifying malicious activities, it also facilitates the assessment of privacy-preserving mechanisms, such as pseudonym change schemes. Pseudonym change schemes are essential in vehicular networks to protect user privacy by periodically altering vehicle identifiers, thereby preventing unauthorized tracking. F2MD enables researchers to simulate various pseudonym change strategies, including time-based and event-based approaches, within realistic vehicular communication scenarios. By integrating these schemes into the simulation framework, F2MD allows for comprehensive analysis of their effectiveness. F2MD implement five different pseudonyms change scheme:

1. Periodical: vehicles change pseudonym every 60 seconds
2. Disposable: vehicles change pseudonym after sending 10 BSMs
3. Distance: vehicles change pseudonym after traveling 80 meters

4. Random: vehicles change pseudonym after each BSM is sent with a probability of 10

5. Car2Car: combination of periodical and distance. Car2Car defines two different policies for pseudonym change. The first policy is used only when changing the pseudonym for the first time, and uses a distance-based solution by changing pseudonym after the vehicle traveled for a random number of meters comprised between 800 and 1500. Then, each subsequent pseudonym change occurs when two conditions are met: the vehicle must have traveled at least 800 meters from the last pseudonym change and a random number of seconds (between 120 and 360 seconds) must have passed since the last pseudonym change.

3 Scenario

The scenario used for the evaluation was generated using SUMO (Simulation of Urban Mobility), which allowed us to realistically simulate vehicular traffic flows, mobility patterns, and driver behaviors in urban environments. The simulation considered various urban configurations, vehicle densities, and road topologies to ensure comprehensive coverage and realistic representation of real-world mobility patterns. SUMO enabled precise control over individual vehicle trajectories, allowing us to closely analyze the interactions between vehicles and communication infrastructures.

To evaluate the effectiveness of pseudonym-change schemes, we selected three representative urban scenarios extracted from real-world Italian cities: Modena (MASA), Pisa, and Catania which correspond to the cities of the other partner of the project. Each scenario represents a small but highly characteristic area of its respective city, chosen for the diversity in urban layouts, traffic densities, and mobility behaviors.

3.1 MASA (Modena Automotive Smart Area) [4] Scenario:

The MASA scenario represents a dedicated urban testbed established in Modena, specifically designed to facilitate research in smart mobility, connected vehicles, and autonomous driving. The selected area includes urban segments with interconnected streets, smart intersections equipped with intelligent traffic lights, obstacle-recognition cameras, and various sensor technologies. Due to its experimental nature, the MASA area allows for comprehensive testing of pseudonym-change mechanisms, particularly evaluating their effectiveness in situations involving frequent vehicle interactions with smart roadside infrastructures. The scenario is characterized by medium traffic densities, organized traffic flows, and systematically instrumented road segments, providing an ideal controlled environment for evaluating advanced vehicular communication and privacy solutions.

3.2 Pisa Scenario:

The Pisa scenario represents a historical city center characterized by narrow streets, dense traffic, complex intersection topologies, and significant pedestrian and cyclist activity. The selected urban segment includes multiple junctions and tight road configurations typical of older European cities. These conditions lead to frequent vehicle stops, starts, and sharp maneuvers, challenging pseudonym-change schemes due to increased correlation opportunities created by frequent events such as intersection stops and turns. Additionally, the dense urban layout results in slower speeds, higher congestion, and more intricate mobility patterns. Consequently, this scenario allowed for rigorous testing of privacy strategies under conditions likely to stress the pseudonym management process significantly.

3.3 Catania Scenario:

The Catania scenario comprises broader avenues, suburban roads, and larger intersections, combining urban and semi-urban traffic conditions. Compared to Pisa, this scenario experiences higher average speeds, more straightforward traffic flows, and fewer sudden stops, but includes multi-lane road segments, roundabouts, and extensive stretches of road. The variability in mobility patterns, characterized by rapid transitions between dense urban traffic and faster-moving suburban segments, provides a realistic and challenging environment to assess the pseudonym-change schemes' adaptability. The diversity in road layouts and traffic dynamics found in the Catania scenario contributes significantly to the evaluation, highlighting the effectiveness and potential weaknesses of pseudonym schemes in mixed mobility environments.

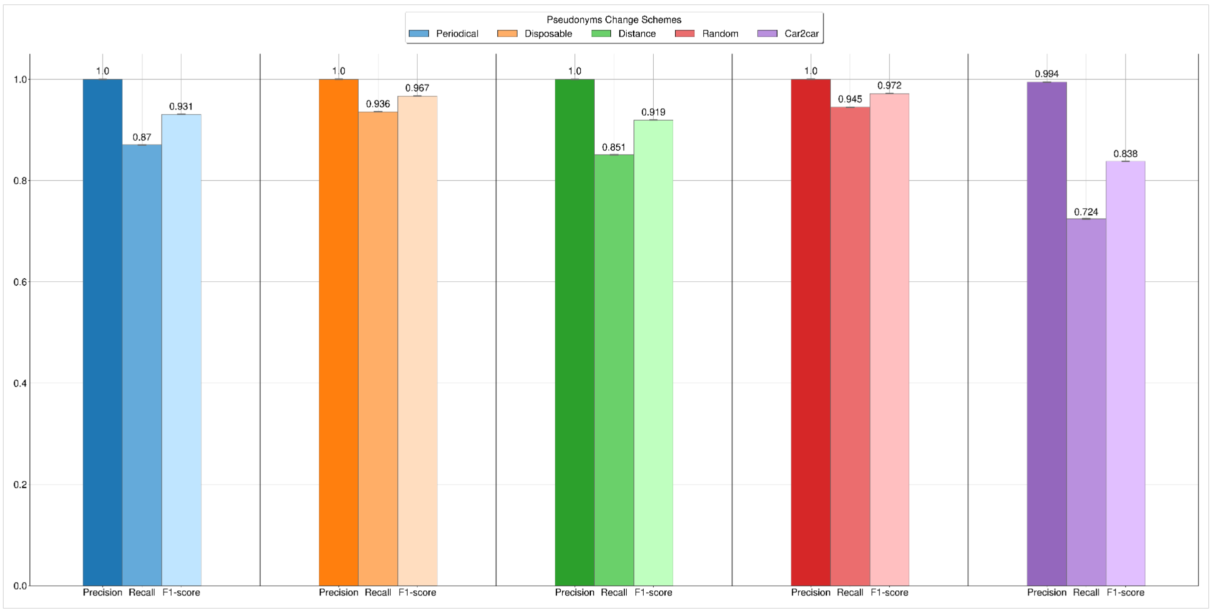

Figure 1: Pseudonyms linking capabilities inside the coverage area of the antenna using 10Hz of sending frequency.

4 Performance evaluation

To evaluate the effectiveness of both attack methodologies proposed in the Deliverable D1.1 we perform different tests depending on the capabilities of the attacker.

4.1 DSRC attacker

To measure the performance of the simpler attack methodology which relies on the pure DSRC communications (Section 4.1 of D1.1) we perform multiple simulations against the pseudonym-change schemes of F2MD described in Section 2.4. We evaluate the performance by means of precision, recall, and F1-score indexes. While the precision is used to measure the ratio of correctly linked pseudonyms over the total of pseudonyms, the recall is used to identify the ratio of correct pseudonym change matched over the total number of changes. The F1 -score index is used as a summary of the tracking performance, considering both precision and recall equally weighted. The performance obtained against all the pseudonyms change schemes are reported in Figure 1, starting from the left is possible to see the Periodical (colored in blue), then the Disposable (colored in orange), followed by the Distance (colored in green), while on the right part there is the Random (colored in red) and the Car2Car (colored in purple). As it is possible to observe from the results, the attacker is able to reach the maximum value of precision against almost all the pseudonyms change schemes. Also, while considering the F1-score the attacker is able to reach values over 0.9 in all the pseudonyms change schemes except for the Car2Car. However, the attacker is able to reach 0.84 against the Car2Car change scheme, which is not sufficient for ensuring privacy in the VANETs communications.

4.2 Multi radio signal attacker

To measure the performance of the more sophisticated attack methodology which relies on multi protocols communications (DSRC and Wi-Fi) (Section 4.2 of D1.1) we perform multiple simulations against the pseudonym-change schemes of F2MD described in Section 2.4.

Due to technical constraints and performance considerations, we limited our analysis to two primary message types. The first type was the Basic Safety Message (BSM) defined by the DSRC protocol (Dedicated Short-Range Communications, IEEE 802.11p). BSMs contain essential information such as vehicle position, speed, acceleration, and heading, making them ideal for tracking and correlation analyses. The second type was the Wi-Fi beacon frame, regularly emitted by vehicle onboard Wi-Fi modules. Wi-Fi beacons include persistent unique identifiers, notably MAC addresses, allowing additional opportunities for vehicle tracking across pseudonym changes.

The performance evaluation compared three different heuristics:

- Count: consider 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 linking performance is evaluated by means of precision (left part), recall (center part) and F1-measure (right part). In all the different parts of both Figure 1 and Figure 2, results related to the Count metric are depicted with the left-most boxplot (colored in red), results related to the Statistical RSSI metric are depicted in the centered boxplot (colored in blue), while results related to the Pearson RSSI are depicted in the right-most boxplot (colored in green).

From the analysis of the results of Figure 1 it is clear that the Pearson RSSI achieves the highest results in both precision and recall, while Count and Statistical RSSI exhibits higher recall with higher variance in their interquartile ranges.

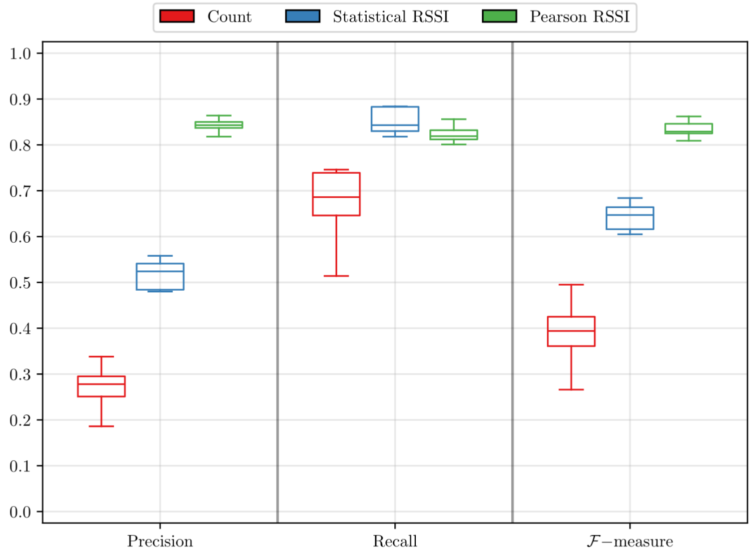

Figure 2: Vehicle linking capabilities between different coverage area of the antennas using 10Hz of sending frequency.

We also remark that both Count and Statistical RSSI metrics have a lower precision compared to the previous scenario, since increasing the sending frequency also increases the false positive rates for these two metrics.

As an example, in Figure 3 we present the portion of the MASA testbed area to demonstrate how an attacker using simple equipment is able to track a vehicle over the different coverage areas by correlating the DSRC's pseudonyms and Wi-Fi probe ID. The black dot of Figure 3 at the center of the three different roundabouts represent the attacker's antenna, while the other colored dots represent the different pseudonyms used by the same vehicle during its traveling.

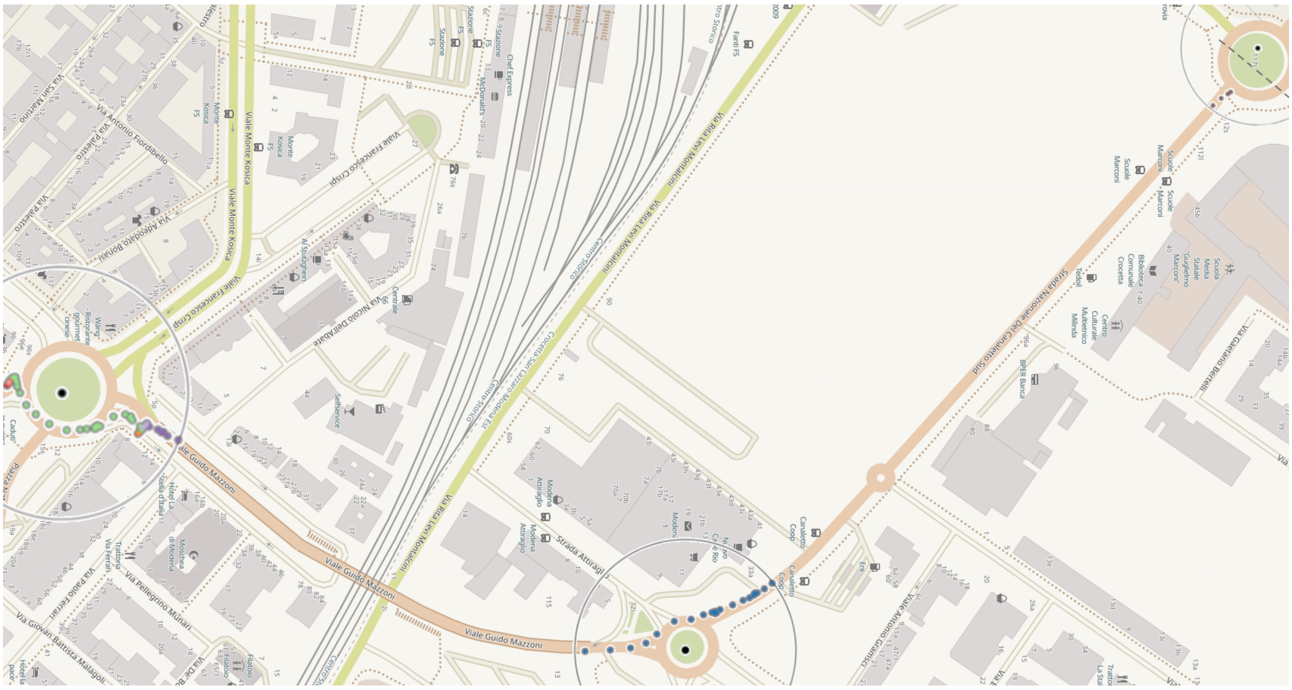

Figure 3: Vehicle trajectory reconstruction.

5 Conclusions

In this work, we analyzed and evaluated the effectiveness of pseudonym-change schemes for enhancing vehicle privacy within Vehicular Ad Hoc Networks (VANETs). By simulating realistic mobility scenarios through the integration of SUMO, OMNeT++, and Veins, we examined three distinct urban areas: the Modena Automotive Smart Area (MASA), Pisa, and Catania. These environments represented diverse urban conditions, enabling comprehensive testing of pseudonym-change strategies under varying traffic densities, road structures, and traffic patterns.

The analysis focused on evaluating the robustness of pseudonym changes employing DSRC Basic Safety Messages (BSMs) and Wi-Fi beacon frames. Our findings demonstrate that pseudonym-change schemes, while providing a certain degree of privacy, are inherently vulnerable, especially when analyzed in conjunction with other vehicular communication signals that broadcast persistent unique identifiers. Higher-frequency message transmissions, essential for safety-critical applications, significantly increased opportunities for tracking and pseudonym linking, underscoring a trade-off between privacy and safety requirements.

References

[1] Michael Behrisch, Laura Bieker-Walz, Jakob Erdmann, and Daniel Krajzewicz. Sumo - simulation of urban mobility: An overview. 2011.

[2] Joseph Kamel, Mohammad Raashid Ansari, Jonathan Petit, Arnaud Kaiser, Ines Ben Jemaa, and Pascal Urien. Simulation framework for misbehavior detection in vehicular networks. *IEEE Transactions on Vehicular Technology*, 2020.

[3] Pablo Alvarez Lopez, Michael Behrisch, Laura Bieker-Walz, Jakob Erdmann, Yun-Pang Flötteröd, Robert Hilbrich, Leonhard Lücken, Johannes Rummel, Peter Wagner, and Evamarie Wiessner. Microscopic traffic simulation using sumo. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018.

[4] University of Modena and Reggio Emilia. MASA - Modena Automotive Smart Area, 2021.

[5] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, 2008.