This is a pre print version of the following article:

Are VANETs pseudonyms effective? An experimental evaluation of pseudonym tracking in adversarial scenario / Gambigliani Zoccoli, G., Stabili, D., Marchetti, M.. - (2023), pp. 1-6. (98th IEEE Vehicular Technology Conference, VTC 2023-Fall Hong Kong, HONG KONG OCT 10-13, 2023) [10.1109/VTC2023-Fall60731.2023.10333561].

Institute of Electrical and Electronics Engineers Inc.
Terms of use:

The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

26/11/2026 11:00

(Article begins on next page)

Are VANETs pseudonyms effective? An experimental evaluation of pseudonym tracking in adversarial scenario

Giovanni Gambigliani Zoccoli*, Dario Stabili† and Mirco Marchetti*
* University of Modena and Reggio Emilia
Department of Engineering "Enzo Ferrari"
{giovanni.gambiglianizoccoli, mirco.marchetti}@unimore.it
† Alma Mater Studiorum - University of Bologna
Department of Computer Science and Engineering
dario.stabili@unibo.it

***Abstract*—With the increasing adoption of Vehicular Ad Hoc Networks (VANETs) for the development of Cooperative Intelligent Transportation Systems (C-ITS) many concerns regarding privacy and anonymity in VANETs have been raised by security researchers and practitioners, highlighting the need for effective mechanisms to protect sensitive information exchanged by connected vehicles. One of the first concerns is related to the vehicle's identifier, a field contained in the messages sent from the vehicle and that can be used to track the vehicle across the infrastructure, with consequent severe implications on the privacy of the driver. Consequently, VANET communications leverage short-lived pseudonyms instead of persistent vehicle's identifiers, aiming to enhance the privacy of the vehicle. Pseudonym change schemes proposed in the literature are effective in masking the real sender of a given message, but they do not guarantee privacy against attackers that can monitor and correlate multiple messages among themselves. This paper evaluates 5 different pseudonym change mechanisms against a realistic threat model. Our results demonstrate that it is possible for a realistic attacker to reliably track multiple vehicles, with minor differences across different pseudonym change schemes.**

I. Introduction

In recent years, the rapid advancement of vehicular technologies has revolutionized the transportation landscape, leading to the emergence of Vehicular Ad Hoc Networks (VANETs). VANETs enable vehicles to communicate with each other and with roadside infrastructure, fostering the development of intelligent transportation systems and enhancing road safety, traffic efficiency, and passenger comfort [1]. However, as these networks become increasingly integrated into our daily lives, concerns regarding privacy and security arise, highlighting the need for effective mechanisms to protect the sensitive information exchanged among vehicles [2].

Numerous academics and industry experts have successfully demonstrated how an attacker, possessing either direct or remote access to in-vehicle communication protocols, can manipulate the proper functioning of drive-by-wire systems [3], [4]. Furthermore, they have introduced cybersecurity solutions specifically designed for safeguarding internal vehicle networks [5], [6] and the entire vehicle system [7]. As a natural progression towards protecting vehicles from unauthorized remote access, it becomes imperative to improve all security aspects of VANETs, including privacy.

VANETs face a intrinsic trade-off between the privacy of drivers, the ability to quickly identify vehicles in case of emergencies, and the need to blame the originator of malicious or incorrect messages. Traditional network protocols and communication architectures often rely on persistent identifiers (IDs) to uniquely identify vehicles, making it possible for an adversary to track and trace a vehicle's movements, ultimately compromising the privacy of drivers and passengers. To avoid that, in VANETs the concept of vehicle pseudonym has gained significant attention as a promising solution to mitigate privacy concerns.

The idea is for each vehicle to replace its persistent and unique vehicle identifier with a short-lived pseudonym that can modified very often according to a given strategy, thus preventing tracking and improving anonymity. By adopting pseudonyms, vehicles can maintain their privacy by decoupling their true identity from the identifiers used for communication purposes. Moreover, pseudonyms can also serve as a defensive measure against various security threats, including impersonation attacks and message injection.

Many different policies for pseudonym change have already been proposed in the literature. However, the majority of these work (see Section III for more details) do not evaluate the effectiveness of the proposed pseudonym change scheme against a realistic attacker aiming to track long journeys by linking multiple different pseudonyms associated to the same vehicle over time.

To fill this gap, in this paper we discuss the effectiveness of 5 popular pseudonym change schemes described and implemented in [8] (the state-of-the-art framework for misbehavior detection) in the presence of a realistic attacker that is able to passively monitor wireless communications from VANETs by using a simple antenna, demonstrating how it is possible to

evade pseudonym change schemes to track a target vehicle.

The rest of this paper is organized as follows. Section II illustrates the basic knowledge required for the understanding of this work, while Section III presents the pseudonym change schemes already available in current literature. Section IV showcase our pseudonym tracking framework, while its performance against the state-of-the-art pseudonym change schemes are presented in Section V. Finally, conclusions and future research directions are outlined in Section VI.

II. Introduction to VANETs

Vehicular Ad-Hoc Networks (VANETs) are dynamic networks formed by vehicles, allowing them to communicate with each other and roadside infrastructure. These networks facilitate real-time information sharing and collaboration among vehicles, with the goal of enhancing road safety, improving traffic efficiency, and offering innovative passenger services. One of the crucial components of VANETs for the future of transportation systems are Cooperative Intelligent Transportation Systems (C-ITS), which aim to integrate advanced communication technologies and intelligent transportation systems to enable cooperative interactions between vehicles and infrastructure. C-ITS enables vehicles to engage in Vehicle-to-Vehicle communication and Vehicle-to-Infrastructure communication, exchanging pertinent data like position, speed, and road conditions. This data empowers vehicles to make informed decisions and cooperate in order to prevent accidents, optimize traffic flow, and enhance the overall transportation experience. The applications and advantages of C-ITS are extensive, encompassing collision warning and avoidance, cooperative adaptive cruise control, intersection management, traffic signal optimization, and intelligent route planning. However, to enable the development of C-ITS it is necessary to define a standard to allow vehicles and other connected entities to participate in the network tackling critical aspects of vehicular communications, such as frequent movement, sporadic connectivity, and ever-changing network structures. One notable communication standard employed in VANETs is *IEEE 802.11p*, commonly known as Wireless Access in Vehicular Environments (WAVE). This extension of the widely used IEEE 802.11 Wi-Fi standard is specifically tailored for vehicular communication. Operating within the 5.9 GHz frequency band, $IEEE802.11p$ enables high-speed and low-latency communication among vehicles and between vehicles and roadside infrastructure.

$IEEE802.11p$ serves as the foundation for various VANET applications, encompassing V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) communication. It leverages dedicated short-range communication (DSRC) technology, facilitating the exchange of safety-critical information among vehicles.

At the protocol's upper layer, the SAE $J2735$ Message Set Dictionary standard defines the Application Layer and includes fifteen distinct message types. Developed by the Society of Automotive Engineers (SAE), the SAE J2735 Message Set Dictionary establishes a comprehensive collection of messages for vehicular communication systems. By providing a standardized format for data elements, message types, and their corresponding definitions, this dictionary ensures interoperability and consistent interpretation of messages across diverse communication platforms. The SAE $J2735$ Message Set Dictionary defines different messaging protocols that can be adopted for the different scenarios of C-ITS communication. One of the most important set of messages is the Basic Safety Message (BSM), typically sent by vehicles periodically to exchange safety-critical information. The frequency at which BSMs are transmitted can vary depending on the specific implementation and requirements of the VANET system. However, a common practice is to send BSMs at regular intervals, typically ranging from 100 to 200 milliseconds. These messages consist of two distinct components: the first part encompasses essential state information present in all BSM messages, while the second part contains optional parameters. The first part, which is divided into 13 fields, includes vital details such as GPS coordinates, braking system status, speed, acceleration, timestamp of the message transmission, and additional information like vehicle dimensions. By disseminating these messages, VANET users engaged in the communication process can enhance safety measures and decrease the response time required for critical actions. To identify those messages, an `identifier` field is included in the first part of the message. To prevent direct tracking of the vehicle from the analysis of the positions of BSMs with the same `identifier`, a pseudonym is used for anonymity of the communication. Despite the adoption of pseudonyms in VANETs to preserve the anonymity of the vehicles, researchers already discussed different pseudonym change schemes to ensure proper preservation of the privacy of the vehicle, preventing any malicious entity to easily track and locate them. However, to the best of our knowledge the privacy preserving capabilities of the different pseudonym change schemes have never been thoroughly tested before, and it is also good practice to not rely on this single mechanism to ensure the privacy of the vehicle in VANETs communication but also to deploy other scenario-specific solutions aimed to strengthen the privacy-preserving abilities in VANETs.

III. Related work

The scientific literature already includes several work aiming at proposing pseudonym change strategies. Unfortunately, some of them are inapplicable since they would require assistance from an intelligent infrastructure that is currently lacking and will likely not be implemented in the future. In this category we include the pseudonym change strategy proposed by the authors of [9], in which vehicles receive a new pseudonym determined by the infrastructure only when crossing predefined "Virtual Locations Privacy Zones" (VLPZ). Pseudonyms are never changed outside of a VLPZ, and cannot be changed autonomously by a vehicle. Another work belonging to this category is proposed by the authors of [10], in which the pseudonyms change scheme requires

the cooperation between vehicles. These motivation led us to exclude these strategies from the current evaluation.

Five different pseudonym change strategies that are deployable without modification to the standard message formats and that do not require cooperation form the infrastructure nor other vehicles are included in the F^2MD framework [8]. This paper considers all these 5 strategies in its evaluation.

Other works that are closely related to our proposal focus on vehicle tracking through pseudonym linking. The first solution in this field is [11]. The approach proposed in this paper is based on a "learning phase" in which the attacker gathers a background truth related to the traffic distribution and travel time of all the vehicles driving within a given area. Moreover, this paper evaluates two pseudonym change strategies: simple "time based" (similar to the *periodical* considered in this work) and the one proposed by [10]. On the other hand, in this work we consider a weaker attacker that cannot build the background truth (we remark that is not clear from [11] how this knowledge can be acquired in a real scenario), and we consider all the 5 strategies included in the F^2MD framework.

Another methodology is presented in [12], that is based on *syntactic* and the *semantic* linking. The former assumes that if only a single vehicle changes pseudonym during a period of time it is possible to link the two pseudonyms to the same vehicle, while the latter requires the prediction of the position of the vehicle and the comparison of the pseudonym used in the BSMs. Moreover, their experimental evaluation is based on the VEINS framework which (in their experiments) uses the pseudonyms changes schemes presented in [13] that leverage on a lower number of fields compared to the pseudonyms changes scheme presented in F^2MD [8].

Another solution investigating possible pseudonym changing schemes is presented in [14], where the authors propose a tracking evaluation of the single C-ITS pseudonyms changes scheme [15]. Moreover, their tracking framework include some optional information of the SAE $J2735$ standard, such as the dimensions of the vehicles.

In this work we propose a novel tracking solution that is compatible with the published IEEE 1609 standard and that does not require statistical ground truth that would be hard to gather for a realistic, limited attacker. Compared to this previous work, in our paper we extend the test of the pseudonym changing scheme on more sophisticated methodologies (described in [8]), presenting a novel benchmark for the evaluation of the effectiveness of pseudonym changing schemes that can be used by security researchers [1].

In conclusion, this work advances the current state-of-the-art by presenting an experimental analysis of the tracking of 5 different pseudonym changing schemes, on a realistic scenario without requiring any modification to the $IEEE1609$ standard.

IV. Pseudonym Tracking Framework

In this section we highlight the design choices of our Pseudonym Tracking Framework (PTF) that we use to verify the privacy-preserving capabilities of the pseudonym change schemes. Our test framework is designed to use the content of BSMs exchanged by vehicles in VANETs for the pseudonym tracking.

Our threat model assumes an attacker having a limited number of antennas that are used to passively collect the messages exchanged by the vehicles within the coverage area of the antennas. The attacker does not need any access to Road Side Units possibly deployed in the area of the attack.

Our tracking solution aims to link pseudonyms that changes within the area of coverage of all the antennas hold by the attacker. In our tracking process, the framework 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 which value is has never been observed before). This association is time-based using the formula:

$$T_{last} < T \leq T_{last} + B_{time} + \Delta_{tol} \tag{1}$$

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, kept as a configuration parameter in our tests), while Δ_{tol} 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 to 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). We remark that it is also possible to identify the most similar vehicle by using the content of the `VehicleSize` field contained in the BSM with precision very close to 100%. However, since this field is not included in the mandatory part of the BSM but is defined as an optional field by the standard, we decide to ignore this information. The algorithm then sorts all the candidate BSMs in ascending distance order, calculated by applying the euclidean distance between the message with the old pseudonym and the ones with the new values. Then, we use the timestamp value and the speed of our target BSM and the timestamp of each candidate BSM for the identification of the best match. The best match is selected as the BSM having an euclidean distance from the original BSM in close proximity (with 2 meters tolerance) to the value obtained by multiplying the timestamp difference between the original message and the candidate one (Δ_{ts}) for the speed of the original BSM ($speed$). If the candidate BSM having the smaller euclidean distance from the original message is not compatible with the traveled distance computed from the original BSM, then it is removed from the candidate list and the algorithm continues with the second closest BSM. This process terminates after the first message complying with our filters is found, thus identifying two different BSMs as related to the same vehicle. The summary of our tracking algorithm is presented in Algorithm 1.

[1] https://github.com/SECloudUNIMORE/ACS

Algorithm 1 Pseudonym tracking

function MATCHPSEUDONYMS($BSMs$)
  $PList_{last} =$ LAST MESSAGE(BSM)
  for p **in** $PList_{last}$ **do**
    $C_{first} =$ FIRST MESSAGE($BSM, T_p, B_{time}, \Delta_{tol}$)
    $OrdList =$ SORTBYDIST(C_{first}, p)
    for c **in** $OrdList$ **do**
      $t_{Dist} = (Ts_p - Ts_c) * Speed_p$
      if $t_{Dist} - 2 \leq dist_c \leq t_{Dist} + 2$ **then** ▷ The best match is found and a link between p and c is created
        $TrackPseudonyms = (p, c)$
        break



Fig. 1: The Modena Automotive Smart Area (red circles indicates the location of the antenna used by the attacker for the tracking of the vehicles)

V. PERFORMANCE EVALUATION OF THE PSEUDONYMS TRACKING FRAMEWORK

A. Simulation scenario

This section presents the experimental evaluation of the PTF presented in this work against the pseudonym change schemes included in the F^2MD framework [8], one of the most used framework for misbehavior detection in VANETs under different circumstances. The F^2MD supports 5 different pseudonym change schemes:

- **Periodical:** vehicles change pseudonym every 60 seconds;
- **Disposable:** vehicles change pseudonym after sending 10 BSMs;
- **Distance:** vehicles change pseudonyms after traveling 80 meters;
- **Random:** vehicles change pseudonym after each BSM is sent with a probability of 10%;
- **Car2Car:** this scheme is designed as a combination of *periodical* and *distance*, and 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.

Our experimental setup is based on the VEINS simulator [16] since we want to test the pseudonym changing schemes supported by the F^2MD framework. VEINS is an open source framework for the simulation of vehicular communication networks based on *OMNet++* [17] and *SUMO* [18]. We simulated the different pseudonym changing schemes deployed in the *Modena Automotive Smart Area* (MASA), where the attacker has already installed three antennas in three roundabouts, as depicted in Figure 1. In our evaluation tests, we use the default configuration of the VEINS simulator of the scenario, thus not limiting the observation radius of our antennas with a fixed threshold, as has been proposed in other proposals [11]. The default VEINS configuration consider a *transmission power* of 100 mW and moreover include a sophisticated obstacle shadowing model which has been calibrated and validated against real world measurements capturing the effect of large building and by blocking the signal transmissions [19], [20].

We tested the tracking capabilities of our system against each pseudonym changing scheme by sending the BSMs with 4 different frequencies: $1, 2, 5$ and 10 Hz. We also remark that in our evaluation tests the B_{time} values of the Formula 1 is considered as the 50% of the period, which is defined as the inverse of the frequency.

The results are presented by means of *precision*, *recall*, and $\mathcal{F}_1$-score indexes, a set of widely used index to measure the quality of the detection. 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 $\mathcal{F}_1$-score index is used as a summary of the tracking performance of our framework, considering both *precision* and *recall* equally weighted. All the three index values range between 0 (poor detection capabilities) and 1 (perfect score).

B. Tracking results

Periodical: Table I summarizes the detection results of our PTF against the *periodical* pseudonym change scheme presented in [8]. The rows of Table I represent the different B_{time} considered in our test scenario, with BSMs sent every (top to bottom) $1000, 500, 200$ and 100 milliseconds; while the columns shows the average (μ) and standard deviation (σ) values of *precision, recall* and $\mathcal{F}_1$-score achieved by our PTF across 5 different simulations.

From the results presented in Table I it is possible to notice that our algorithm achieves precision values higher than 0.99 against all the different B_{time} values considered in our tests, thus being able to precisely identify the pseudonym change independently from the send frequency of a BSM. In particular, our solution is also able to achieve high $\mathcal{F}_1$-score values

B_{time} $[ms]$	Precision $\mu[\sigma]$	Recall $\mu[\sigma]$	$\mathcal{F}_1$-score $\mu[\sigma]$
1000	0.9952 [0.0015]	0.9090 [0.0109]	0.9502 [0.0064]
500	0.9989 [0.0005]	0.8676 [0.0168]	0.9285 [0.0097]
200	0.9997 [0.0002]	0.9161 [0.0146]	0.9561 [0.0080]
100	0.9999 [0.0002]	0.8705 [0.0115]	0.9307 [0.0066]

TABLE I: Detection results against the *periodical* pseudonym changing schemes for the different values of B_{time}

.

(≥ 0.92) against the considered pseudonym change scheme, resulting in the poor efficiency of this pseudonym scheme in preserving the anonymity of the communication. However, we remark that despite the overall values of *precision, recall* and $\mathcal{F}_1$-score are always high, by increasing the number of messages (i.e. with lower B_{time}) the *recall* value is lower due to the introduction of false negatives, thus slightly deflecting the $\mathcal{F}_1$-score values.

Disposable: Table II summarizes the detection results of our PTF against the *disposable* pseudonym change scheme. Table II is organized as Table I.

B_{time} $[ms]$	Precision $\mu[\sigma]$	Recall $\mu[\sigma]$	$\mathcal{F}_1$-score $\mu[\sigma]$
1000	0.9979 [0.0017]	0.9837 [0.0043]	0.9907 [0.0017]
500	0.9992 [0.0002]	0.9333 [0.0129]	0.9651 [0.0069]
200	0.9992 [0.0001]	0.9329 [0.0121]	0.9652 [0.0065]
100	0.9999 [0.0001]	0.9358 [0.0105]	0.9668 [0.0056]

TABLE II: Detection results against the *disposable* pseudonym changing schemes for the different values of B_{time}

.

From the analysis of the results presented in Table II it is clear that our PTF is able to track pseudonym changes with high precision (≥ 0.99) and high $\mathcal{F}_1$-score (≥ 0.96) independently from the send frequency of the BSMs. Moreover, we highlight that the same inverted behavior between the increasing number of messages (i.e. lower values of B_{time}) and a small reduction of $\mathcal{F}_1$-score can be observed as a consequence of the increasing number of false positives.

Distance: Table III summarizes the detection results of our PTF against the *distance* pseudonym change scheme. Table III is organized as Table I and II).

B_{time} $[ms]$	Precision $\mu[\sigma]$	Recall $\mu[\sigma]$	$\mathcal{F}_1$-score $\mu[\sigma]$
1000	0.9854 [0.0030]	0.8254 [0.0055]	0.8983 [0.0025]
500	0.9938 [0.0018]	0.6410 [0.0152]	0.7792 [0.0116]
200	0.9998 [0.0003]	0.8801 [0.0099]	0.9360 [0.0055]
100	0.9999 [0.0002]	0.8510 [0.0053]	0.9194 [0.0030]

TABLE III: Detection results against the *distance* pseudonym changing schemes for the different values of B_{time}

.

From the analysis of the results presented in Table III it is possible to notice that, also against this pseudonym change scheme, our PTF is able to achieve values of *precision* higher than 0.98, resulting in $\mathcal{F}_1$-score higher than 0.77 in all the different B_{time} scenarios considered in our test. However, contrary to the two previous results, by increasing the number of messages (i.e. lower value of B_{time}) in this pseudonym change scheme our PTF is able to increase the overall tracking performance, reaching $\mathcal{F}_1$-score values higher than 0.91 with B_{time} equal to 200 and 100 milliseconds.

Random: Table IV summarizes the detection results of our PTF against the *random* pseudonym change scheme. Table IV is organized as the previous tables of this section, highlighting how the send frequency of a BSM (B_{time}) affects the tracking capabilities of our PTF.

B_{time} $[ms]$	Precision $\mu[\sigma]$	Recall $\mu[\sigma]$	$\mathcal{F}_1$-score $\mu[\sigma]$
1000	0.9980 [0.0013]	0.9393 [0.0177]	0.9677 [0.0091]
500	0.9993 [0.0004]	0.9093 [0.3563]	0.9522 [0.3349]
200	0.9999 [0.0001]	0.8691 [0.0046]	0.9299 [0.0026]
100	0.9999 [0.0001]	0.9449 [0.0018]	0.9717 [0.0016]

TABLE IV: Detection results against the *random* pseudonym changing schemes for the different values of B_{time}

.

From the analysis of the results presented in Table IV it is possible to notice that our PTF is able to achieve high *precision* (≥ 0.998) and high $\mathcal{F}_1$-score values (≥ 0.92). However, as opposed to the previous attack scenarios, in the *random* pseudonym change scheme our tracking algorithm performance does not exhibit a particular behavior related to the send frequency of the BSMs.

Car2Car: Table V summarizes the detection results of our PTF against the *car2car* pseudonym change scheme. Table V is organized as the previous tables of this section, highlighting how the send frequency of a BSM (B_{time}) affects the tracking capabilities of our PTF.

B_{time} $[ms]$	Precision $\mu[\sigma]$	Recall $\mu[\sigma]$	$\mathcal{F}_1$-score $\mu[\sigma]$
1000	0.9794 [0.0155]	0.7128 [0.0513]	0.8242 [0.0358]
500	0.9795 [0.0116]	0.7314 [0.0714]	0.8359 [0.0499]
200	0.9971 [0.0055]	0.7129 [0.0296]	0.8309 [0.0182]
100	0.9944 [0.0038]	0.7245 [0.0252]	0.8381 [0.0200]

TABLE V: Detection results against the *car2car* pseudonym changing schemes for the different values of B_{time}

.

From the results presented in Table V it is possible to notice that the *precision* and *recall* achieved with our PTF against the *Car2Car* pseudonym change scheme express little to no variance, hence resulting in $\mathcal{F}_1$-score ranging 0.8242 to a maximum of 0.8381. Compared to the previous performance of our tracking algorithm, we remark that against this attack scenario the tracking performance of our algorithm are not influenced by the send frequency of the BSMs.

VI. Conclusions

In this work we present a methodology for tracking pseudonyms in VANETs, describing how a limited attacker can break the anonymity in VANETs communication by only using

the mandatory content of the BSMs standard. Our solution is based on the simple assumption that the attacker has the ability to install passive antennas to gather BSMs sent by vehicles during normal VANETs communications. We also present an experimental evaluation of our tracking algorithm against 5 state-of-the-art pseudonym changing schemes included in F^2MD. Our results show that all strategies are vulnerable. In particular, for a sending frequency of 10Hz 4 out of 5 strategies can be tracked with a $\mathcal{F}_1$-score higher than 91% (up to 97% for the random strategy), while *Car2Car* exhibit a better behavior with a $\mathcal{F}_1$-score of 83%.

In light of these results, we believe future works focused on the proposal of pseudonym changing schemes for VANETs should consider our Pseudonym Tracking Framework to evaluate the effectiveness of future pseudonym changing schemes for VANETs communication. To this aim, we publicly release our PTF algorithm[1].

ACKNOWLEDGEMENTS

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

This work has been supported by the project "FuSeCar" funded by the MUR Progetti di Ricerca di Rilevante Interesse Nazionale (PRIN) Bando 2022 - grant 2022W3EPEP.

REFERENCES

[1] C. K. Toh, "Ad hoc wireless networks: Protocols and systems," USA, Tech. Rep., 2001.

[2] A. Paul, N. Chilamkurti, A. Daniel, and S. Rho, "Chapter 2 - intelligent transportation systems," in *Intelligent Vehicular Networks and Communications*. Elsevier, 2017.

[3] C. Miller and C. Valasek. (2014) Adventures in automotive networks and control units.

[4] ——. (2015) Remote exploitation of an unaltered passenger vehicle. White paper of Blackhat US conference. [Online]. Available: http://illmatics.com/Remote%20Car%20Hacking.pdf

[5] D. Stabili, L. Ferretti, M. Andreolini, and M. Marchetti, "Daga: Detecting attacks to in-vehicle networks via n-gram analysis," *IEEE Transactions on Vehicular Technology*, vol. 10, p. 15, 2022.

[6] F. Pollicino, D. Stabili, and M. Marchetti, "Performance comparison of timing-based anomaly detectors for controller area network: A reproducible study," *ACM Trans. Cyber-Phys. Syst.*, jun 2023, just Accepted. [Online]. Available: https://doi.org/10.1145/3604913

[7] D. Stabili, R. Romagnoli, M. Marchetti, B. Sinopoli, and M. Colajanni, "A multidisciplinary detection system for cyber attacks on powertrain cyber physical systems," *Future Generation Computer Systems*, vol. 144, p. 151 – 164, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149888496&doi=10.1016%2fj.future.2023.02.019&partnerID=40&md5=b422c78306d2e24808c30688f0a612cd

[8] J. Kamel, M. Ansari, J. Petit, A. Kaiser, I. Ben Jemaa, and P. Urien, "Simulation framework for misbehavior detection in vehicular networks," *IEEE Transactions on Vehicular Technology*, 2020.

[9] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "PRIVANET: An efficient pseudonym changing and management framework for vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 8, pp. 3209–3218, Aug. 2020. [Online]. Available: https://doi.org/10.1109/tits.2019.2924856

[10] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in vanets," in *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*. IEEE, 2009, pp. 648–652.

[11] D. Förster, F. Kargl, and H. Löhr, "A framework for evaluating pseudonym strategies in vehicular ad-hoc networks," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2015, pp. 1–6.

[12] P. K. Singh, S. N. Gowtham, T. S, and S. Nandi, "CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs," *Vehicular Communications*, vol. 20, p. 100183, Dec. 2019. [Online]. Available: https://doi.org/10.1016/j.vehcom.2019.100183

[13] K. Emara, "Poster: PREXT: Privacy extension for veins VANET simulator," in *2016 IEEE Vehicular Networking Conference (VNC)*. IEEE, Dec. 2016. [Online]. Available: https://doi.org/10.1109/vnc.2016.7835979

[14] S. Escher, M. Sontowski, K. Berling, S. Kopsell, and T. Strufe, "How well can your car be tracked: Analysis of the european c-ITS pseudonym scheme," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. IEEE, Apr. 2021. [Online]. Available: https://doi.org/10.1109/vtc2021-spring51267.2021.9449078

[15] *ETSI, TR 103 415 (v1.1.1) - Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management*, 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf

[16] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved ivc analysis," *IEEE Transactions on Mobile Computing*, 2011.

[17] A. Varga and R. 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*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[18] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. WieBner, "Microscopic traffic simulation using sumo," in *The 21st IEEE International Conference on Intelligent Transportation Systems*, 2018.

[19] C. Sommer, D. Eckhoff, and F. Dressler, "Ivc in cities: Signal attenuation by buildings and how parked cars can improve the situation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1733–1745, 2014.

[20] C. Sommer, D. Eckhoff, R. German, and F. Dressler, "A computationally inexpensive empirical model of ieee 802.11p radio shadowing in urban environments," in *2011 Eighth International Conference on Wireless On-Demand Network Systems and Services*, 2011, pp. 84–90.

[1] https://github.com/SECloudUNIMORE/ACS