RADAR: a Radio-based Analytics for Dynamic Association and Recognition of pseudonyms in VANETs

Giovanni Gambigliani Zoccoli, Filip Valgimigli, Dario Stabili, Mirco Marchetti
University of Modena and Reggio Emilia
Department of Engineering "Enzo Ferrari"
{giovanni.gambiglianizoccoli, filip.valgimigli, dario.stabili, mirco.marchetti}@unimore.it

***Abstract*—This paper presents RADAR, a tracking algorithm for vehicles participating in Cooperative Intelligent Transportation Systems (C-ITS) that exploits multiple radio signals emitted by a modern vehicle to break privacy-preserving pseudonym schemes deployed in VANETs. This study shows that by combining Dedicated Short Range Communication (DSRC) and Wi-Fi probe request messages broadcast by the vehicle, it is possible to improve tracking over standard de-anonymization approaches that only leverage DSRC, especially in realistic scenarios where the attacker does not have full coverage of the entire vehicle path. The experimental evaluation compares three different metrics for pseudonym and Wi-Fi probe *identifier* association (*Count*, *Statistical RSSI*, and *Pearson RSSI*), demonstrating that the *Pearson RSSI* metric is better at tracking vehicles under pseudonym-changing schemes in all scenarios and against previous works. As an additional contribution to the state-of-the-art, we publicly release all implementations and simulation scenarios used in this work [1].**

I. Introduction

In recent years, the rapid growth of vehicular technologies has led to the development of new solutions for improving road safety, traffic efficiency, and driver experience. The most promising solution is Vehicular Ad Hoc Networks (VANETs), a key technology for modern Cooperative Intelligent Transportation Systems (C-ITS) [2], which allow entities participating in the C-ITS to share their status and other data via the Dedicated Short Range Communication (DSRC) protocol [3], [4].

Despite their great potential for enabling future smart cities, VANETs require all entities to share large amouns of information that could be used to profile users, thus exposing them to targeted attacks. As an example, many VANETs applications require connected vehicles to share messages containing their precise location, thus allowing an adversary to track all the habits of their victims.

To mitigate these risks, practitioners from both academia and industry have developed privacy-preserving mechanisms that are currently being adopted in VANETs communication. One of these solutions allows entities to hide their real identity by means of pseudonyms [5], [6], temporary identifiers that are used in VANETs messages to preserve the real identity of the participating entities. Several pseudonym change schemes have been proposed in the literature [7], however this approach is still not sufficient to prevent de-anonimization and tracking of vehicles.

In [8], the authors demonstrated the possibility to track the same vehicle despite the use of different pseudonym-changing schemes, by analyzing data such as position, speed, and acceleration with basic motion and trajectory formulas.

A. Motivations

While existing research on vehicle tracking in VANETs under pseudonym-changing schemes has demonstrated the feasibility of linking pseudonyms [8], [9], all the available approaches rely on strong and often unrealistic assumptions about the attacker's capabilities, typically requiring access to all VANET communications and a complete coverage of the full paths of tracked vehicles. We remark that these assumptions are not practical (especially in large-cities scenarios). Since the effectiveness of the attack is limited to the areas monitored by the attacker, this de-anonymization approach poses a limited threat for real-world deployments.

To address this gap, in this paper we propose RADAR, a Radio-based Analytics for Dynamic Association and Recognition of pseudonyms in VANETs. RADAR considers a more realistic threat model, where the adversary only has access to radio-based communications monitored with antennas that are placed on few non-overlapping areas. RADAR uses two primary sources of signals generated by a connected vehicle: DSRC (as already analyzed in [8]) and Wi-Fi. Wi-Fi is often used in modern In-Vehicle Infotainment (IVI) systems and is commonly found on any personal device of the passengers of the vehicle. Experimental evaluation against existing methodologies and different pseudonym-changing schemes demonstrates the effectiveness of RADAR in tracking vehicles under pseudonym-changing schemes, urging the development of more efficient schemes to preserve the privacy of drivers in VANETs.

B. Contributions

The contributions of this work to the state-of-the-art are threefold. First, we introduce a novel tracking methodology that enables an attacker to monitor vehicles participating

in VANET communications by leveraging multiple radio-based technologies. This approach allows effective vehicle tracking even when the attacker does not have access to all transmitted messages, thereby exposing the limitations of current pseudonym-changing schemes in preserving user privacy. Second, we conduct an experimental evaluation of three distinct tracking metrics, assessing their effectiveness against 5 different pseudonym-changing schemes. We further compare the best-performing metric with existing methods, demonstrating that our approach outperforms prior work across various scenarios. Third, we release the full implementation and simulation setups used in our evaluation [1]. To the best of our knowledge, this is the first publicly available implementation of a vehicle tracking methodology. We hope this contribution will serve as a foundation for future research and encourage further experimental advancements in this area.

C. Manuscript Organization

The rest of this paper is organized as follows. Section II reviews existing literature in the vehicle-tracking field, while Section III provides the required knowledge necessary for understanding of this work. Section IV introduces the design and implementation of RADAR, discussing the supported metrics, while Section V presents the experimental evaluation and comparison of our methodology with previous work. Finally, Section VI summarizes the contributions of this work.

II. Related work

Most related work focuses on presenting a novel pseudonym-changing scheme, with only a few references discussing the effectiveness of these schemes and their resilience against de-anonymization attacks.

The first significant analysis is presented in [10], where the authors analyzed and classified several pseudonym-changing schemes into two main categories: *mix-zone* and *mix-context*. The former includes methodologies that use the vehicle's location to change the pseudonym, while the latter involves approaches that decide whether a pseudonym change is necessary based on different input factors. In [10], the authors also provided an analysis of selected pseudonym-changing schemes aimed at preserving driver privacy in a simulated environment. They highlighted that the only schemes harder to track in such an environment are those based on radio silence. Although these schemes are effective at hiding pseudonym changes in VANET communication by introducing a period of radio silence [9], they have also been criticized for being incompatible with safety-related applications. As a result, many practitioners do not recommend their use in real-world scenarios [11].

Another methodology evaluated as effective in preserving the privacy of VANET users is presented in [12]. Specifically, the authors propose a *Cooperative Pseudonym Exchange and Scheme Permutation (CPESP)*, a technique based on a dual approach to enhance privacy. This methodology can be applied in two distinct scenarios. In the first, CPESP requires a high number of vehicles and changes the pseudonyms of all participating entities simultaneously to reduce traceability. In the second scenario, CPESP operates in environments with fewer vehicles by randomly employing either a silence period or a periodic pseudonym-change scheme. Experimental evaluation against the same attack scenario described in [13] demonstrates the effectiveness of this approach in protecting user privacy. However, all the aforementioned studies present only an experimental evaluation of their proposed pseudonym-changing schemes against a single malicious entity, without comparing their results to alternative tracking methodologies or providing a benchmark for evaluation. Recent works, such as [14], [15], focus on analyzing and mitigating the privacy risks associated with physical-layer signal characteristics demonstrating how Radio Frequency Fingerprinting (RFF) can be exploited by an attacker to track users based on the characteristics of the physical devices. The authors also introduce *FingerJam*, a novel approach that employs controlled low-power jamming to obfuscate device-specific signal features, thereby obstructing RFF-based identification without compromising communication quality. While both approaches contribute valuable insights into physical-layer privacy preservation, they differ from our work, which focuses on analyzing message content and Received Signal Strength Indicator (RSSI) values rather than physical-layer signal characteristics.

The first paper presenting a benchmark comparison of the effectiveness of pseudonym-changing schemes against a malicious actor is presented in [8], where the authors presented an evaluation of the effectiveness of privacy-preserving schemes included in [16] (the reference framework for security and privacy studies on VANET communication). The results presented in [8] demonstrate that complex pseudonym-changing schemes do not provide more robust privacy guarantees, with an attacker with access to VANETs communication being able to track the same vehicle under different pseudonyms with $\mathcal{F}_1$-measure higher than 0.91. However, the tracking framework presented in [8] only considers an attacker accessing all VANET communication as its threat model, thus limiting the attacker tracking capabilities on the only area covered by its antenna.

To address this issue, in this work we propose a novel approach for tracking VANETs communication that considers a more realistic threat model where the attacker is able to monitor multiple radio-based communications with distinct and non-overlapping antennas over a wider area of the target city. In particular, the methodology presented in this work exploits the DSRC protocol used in VANETs communication and the Wi-Fi probing messages generated by the In-Vehicle Infotainment system of a modern vehicle. To the best of our knowledge, this work is the first one presenting a methodology for dynamic association and recognition of pseudonyms based on multiple radio-based communication protocols.

III. Background Knowledge

In this section we present the basic knowledge required to understand the rest of this manuscript. In Section III-A, we

provide the details of VANETs communication and the current methodologies to ensure privacy of the communications; while in Section III-B, we present the fundamentals of the Wi-Fi protocol that are exploited by RADAR to track vehicles in VANETs.

A. VANETs, DSRC and Pseudonyms

VANETs are dynamic networks that enable vehicles to exchange real-time data with each other and with infrastructure, aiming to improve road safety, traffic efficiency, and user experience. At their core lies C-ITS, which supports V2V and V2I communication through frequent data exchange (e.g., position, speed, road conditions) to enable cooperative and informed driving decisions.

Effective C-ITS deployment relies on standardized protocols to handle challenges like high mobility and dynamic topology. The primary standard is IEEE *802.11p*, also known as WAVE, which operates in the 5.9 GHz band with a 23 dBm power limit (200 mW [17], [18]) and enables low-latency communication via DSRC.

At the application layer, SAE J2735 defines the Basic Safety Message [19] (BSM), broadcast by vehicles every $100 - \breve{}200$ ms. BSMs include mandatory state information (e.g., GPS, speed, braking) and optional data for enhanced functionality. Each BSM also includes an identifier field, which is expected to contain the digital identity of the entity sending the message to enable identification. However, many researchers expressed privacy concerns related to the usage of an identifier in a broadcast-type network, developing numerous strategies to reduce tracking risks and protect sensitive user information. One of the most promising solutions to this issue is represented by certificate pseudonyms, a set of pre-loaded, certified public keys stored in the vehicle [10], which are used instead of a static identifier. While the usage of pseudonyms is supported by multiple VANETs standards (such as IEEE [20] and ETSI [21]), there is no a standard procedure describing how pseudonyms should change, thus leading to a variety of pseudonym-changing schemes being proposed by researchers.

Basic pseudonym-changing strategies are often based on parameters such as elapsed time, number of messages sent, or distance traveled [16]. More advanced approaches use contextual factors (such as the presence of nearby vehicles) to trigger changes [6], [16], [22]. Despite the variance of the proposed schemes presented in literature, there are still two major issues that are not covered by previous research. First, several proposals require modifications to the standard BSM structure [22]–[25], making them non-compliant with the IEEE 1609 standard. The second and most critical issue is the lack of evaluation of pseudonym-changing schemes against realistic adversaries. In fact, while many works only present a novel pseudonym-changing scheme to demonstrate its feasibility from a computation perspective, only a couple of existing works have discussed the privacy-preserving effectiveness of existing methodologies [8], [12], despite using an unrealistic and impractical adversarial model.

B. Wi-Fi

The Wi-Fi protocol standard, defined in the IEEE 802.11 standard [26], is a wireless communication protocol enabling high-speed data transfer across short to medium distances. Operating in unlicensed frequency bands, primarily 2.4 GHz and 5 GHz, Wi-Fi employs techniques such as *Orthogonal Frequency Division Multiplexing* (OFDM) to achieve efficient and reliable data transmission. The Wi-Fi protocol supports various modulation schemes and channel widths, allowing for flexible deployment across a range of environments and applications, enabling internet access, media streaming, IoT connectivity, and device-to-device communication.

Modern IVI systems offer Wi-Fi communication to the vehicle's passengers, as either a simple hotspot for sharing cellular connectivity or for more complex applications. Hence, it is now common to find integrated cellular modems in the Telecommunication Units (TCUs) of a modern IVI system, which offer the same features found in a typical wireless access point. As described in the Wi-Fi $IEEE$ 802.11 protocol [26], when a personal device wants to identify the list of nearby available Wi-Fi networks, it sends a broadcast Wi-Fi probe request. Upon reception of the probe request, the IVI system (if the hotspot feature is enabled) responds with a probe response frame, containing all data required by the client to connect to the Wi-Fi access point. This probe response contains 34 different fields, with the most important being:

- `Service Set Identifier (SSID)`: the name of the network as set by the access point;
- `Media Access Control (MAC)`: the physical address of the device broadcasting the Wi-Fi probe.

To prevent loss of probe response, each access point is usually configured to send these messages with a default period of $100\ ms$, with a maximum transmission power equal to $20\ dBm$ (equivalent to $100\ mW$).

IV. Design and implementation of RADAR

In this section we describe the design and the implementation of RADAR. Our tracking algorithm relies on three metrics for linking the messages sent by the vehicles to the unique *identifier* exposed by the Wi-Fi access point in Section III-B. Our threat model considers an attacker with a limited number of antennas to passively monitor VANET communication (i.e., DSRC messages) and Wi-Fi probes received in proximity to the antennas. We remark that this threat model is extremely cost-efficient, since by placing antennas strategically it is possible to track many vehicles even without covering their whole paths.

For tracking vehicles' pseudonyms we employ the same strategy presented in the Pseudonym Tracking Framework [8] (PTF), which is extremely effective in linking the different pseudonyms belonging to the same vehicle inside the coverage area of a single antenna, with peak performance of 0.9 $\mathcal{F}_1$-measure against multiple pseudonym-changing schemes. However, PTF performance drops in a realistic scenario in which the attacker monitors multiple and non-overlapping areas of

the map. The motivation is that PTF cannot link vehicles whose pseudonym changes outside of the area covered by the attacker. Figure 1 shows the clear drop in performance from the "single-zone" scenario considered by the related work [8] (gray points showing high $\mathcal{F}_1$-measure) to the "multi-zone" scenario considered in this work (the $\mathcal{F}_1$-measure over different runs is shown by the orange box-plots). The detailed explanation of the pseudonym-changing schemes used in the comparison presented in Figure 1 is available in the original manuscripts [8], [16].

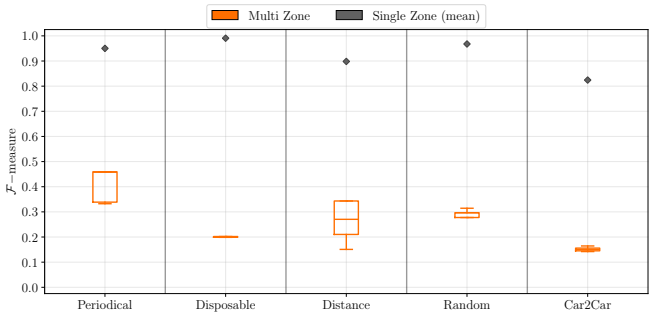

Fig. 1: Multi-zone and single-zone performance comparison of PTF against different pseudonym-changing schemes of F^2MD with 1 Hz of sending frequency

As an effort to overcome this limitation, the tracking methodology developed in this work leverages Wi-Fi probe *ID* of the vehicle's access point as an additional source of information to track a vehicle. We remark that this methodology can be extended to include any other wireless communication protocol (such as Bluetooth Address [27] or TPMS [28]).

The analysis presented in RADAR comprises three phases. In the first phase we use the same strategy presented in PTF [8] to identify all the different pseudonyms associated with the same vehicle inside a single coverage area.

In the second phase we define a list of candidate Wi-Fi probe *IDs* by selecting all the IDs that are received by the antenna within the same time frame as the pseudonyms associated to the same vehicle by PTF. At the end of the second phase we associate a single Wi-Fi probe *ID* to each vehicle within each coverage area. In this work we will evaluate and compare (in Section V) the performance of three different heuristics:

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

Finally, in the third phase of RADAR we use the Wi-Fi probe *ID* to reconstruct the trip of the vehicles across multiple non-overlapping areas.

The full pseudo-code description of RADAR is summarized in Algorithm 1.

Algorithm 1 Vehicle tracking

```
function MatchVehicle(BSMs)
    P_groups = MatchPseudonyms(BSMs)
    for seq in P_groups do
        BMS_msg = GetMessages(seq)
        b_match = FindMatch(
                      unique_ids, BSM_msg, metric)
        LinkVehicle(b_match, BSM_msg)
```

The details of the three different metrics are presented in the next sections.

A. Count metric

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

B. Statistical RSSI metric

The *Statistical RSSI* metric uses the signal strength of the different messages (DSRC and Wi-Fi beacons) for the correlation of the pseudonyms and a unique Wi-Fi probe *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 values of DSRC messages) with different weights associated for every index. The list of indexes and their corresponding weights are 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

We remark that these weights are selected following an experimental validation phase to maximizes the performance of this metric. The detailed description of the RSSI metric is presented in Algorithm 2.

C. Pearson RSSI metric

The *Pearson RSSI* metric uses a more sophisticated approach based on the *Pearson* correlation [29] for the selection of the Wi-Fi probe *ID* corresponding to the reference pseudonyms. We use the correlation between the pure RSSI values collected for the DSRC messages and the Wi-Fi beacon, and associate a list of pseudonyms with the Wi-Fi probe *ID* exhibiting the highest value of Pearson coefficient. We remark that a preliminary step of interpolation is required

Algorithm 2 RSSI metric

function FINDMATCH($unique_{ids}$, $BSMs$, $RSSI$)
  $BSM_{rssi} = \text{GETRSSI}(BSMs)$
  $mean_{dsrc} = \text{MEAN}(BSM_{rssi})$
  $std_{dsrc} = \text{STD}(BSM_{rssi})$
  $median_{dsrc} = \text{MEDIAN}(BSM_{rssi})$
  $min_{dsrc} = \text{MIN}(BSM_{rssi})$
  $max_{dsrc} = \text{MAX}(BSM_{rssi})$
  $mints_{dsrc} = \text{MINTS}(BSM_{rssi})$
  $maxts_{dsrc} = \text{MAXTS}(BSM_{rssi})$
  for u **in** $unique_{ids}$ **do**
    $b = \text{GETMESSAGES}(u)$
    $statistics[u].append(mean_{dsrc} - \text{MEAN}(b))$
    $statistics[u].append(std_{dsrc} - \text{STD}(b))$
    $statistics[u].append(median_{dsrc} - \text{MEDIAN}(b))$
    $statistics[u].append(min_{dsrc} - \text{MIN}(b))$
    $statistics[u].append(max_{dsrc} - \text{MAX}(b))$
    $statistics[u].append(mints_{dsrc} - \text{MINTS}(b))$
    $statistics[u].append(maxts_{dsrc} - \text{MAXTS}(b))$
    $statistics[u] = \text{AVGWEIGHTS}(statistics[u],\ weights)$
  $b_{match} = \text{GETMINIMUM}(statistics)$
  return b_{match}

to align the length of samples in the two sequences. The detailed description of the *Pearson RSSI* metric is presented in Algorithm 3.

Algorithm 3 Improved RSSI metric

function FINDMATCH($unique_{ids}$, $BSMs$, $RSSI$)
  $DSRC_{rssi} = \text{GETRSSI}(BSMs)$
  $DSRC_{rssi} = \text{INTERPOLATE}(DSRC_{rssi})$
  for u **in** $unique_{ids}$ **do**
    $u_{rssi} = \text{GETRSSI}(u)$
    $u_{rssi} = \text{INTERPOLATE}(u_{rssi})$
    $pearson[u].append(\text{PEARSON}(u_{rssi},\ DSRC_{rssi}))$
  $b_{match} = \text{GETBESTMATCH}(pearson)$
  return b_{match}

V. Performance Evaluation

In this section, we present the performance evaluation of RADAR. In Section V-A we present the simulation scenario used in our evaluation, providing all the required details to replicate our experiments. Then, in Section V-B we compare the tracking performance of the three different metrics of RADAR. Finally, in Section V-C we compare the results of the best-performing metric of RADAR against previous work.

A. Simulation scenario

The simulation scenario used to demonstrate the effectiveness of RADAR is based on a modified version of the F^2MD framework [16], a widely used platform for misbehavior detection in VANETs under various scenarios. To simulate a realistic environment, we extended the framework to support the Wi-Fi probing protocol discussed in Section III-B. The experimental setup is based on the VEINS simulator [30], an open-source framework for simulating vehicular communication networks, built on *OMNeT++* [31] and *SUMO* [32]. We simulated the *Modena Automotive Smart Area* (MASA) with a total of 500 vehicles over 20 minutes of simulation, where the attacker had deployed three antennas at three intersections, as shown in Figure 2 [33].

Fig. 2: Graphical representation of the area covered by the attacker (red circles) inside the MASA

To replicate the realistic behavior of real communication networks, we increased the *transmission power* from 100 mW to 200 mW, as explained in [17]. We also enabled the VEINS obstacle shadowing model to capture the impact of large buildings and other obstructions on signal transmission [34], [35].

Since BSMs can be sent with different time intervals depending on the scenario, we tested the tracking performance of RADAR in the worst-case scenario where the lowest number of messages is received, using a sending frequency of 1 Hz. We performed 25 tests overall to remove any possible bias from the results. Moreover, to simulate a simple attacker with access to commonly available equipment, the radius of each monitoring antenna is set to 50 $meters$, thus limiting the monitoring capabilities of the attacker.

Results are depicted by means of $\mathcal{F}_1$-measure, expressing the harminc mean between the precision and the recall of the tracking capabilities of RADAR, with values ranging from 0 (no tracking at all) to 1 (perfect tracking of all entities).

B. Experimental Evaluation

The experimental evaluation presented in this section focuses on the comparison of the proposed heuristics (see Section IV) against the different pseudonym-changing schemes supported in the F^2MD Framework [16]. Figure 3 shows the experimental results of RADAR in the worst-case scenario, where BSMs are sent with a frequency of 1 Hz. We compare the tracking performance of the *Count* (Section IV-A) (depicted in red), the *Statistical RSSI* (Section IV-B) (depicted in blue), and *Pearson RSSI* (Section IV-C) (depicted

in green) metrics against 5 different pseudonym-changing schemes (left-to-right): *Periodical*, *Disposable*, *Distance*, *Random*, and *Car2Car*. The results are depicted by using of box-plots to highlight the variance of the tracking performance between the different metrics.

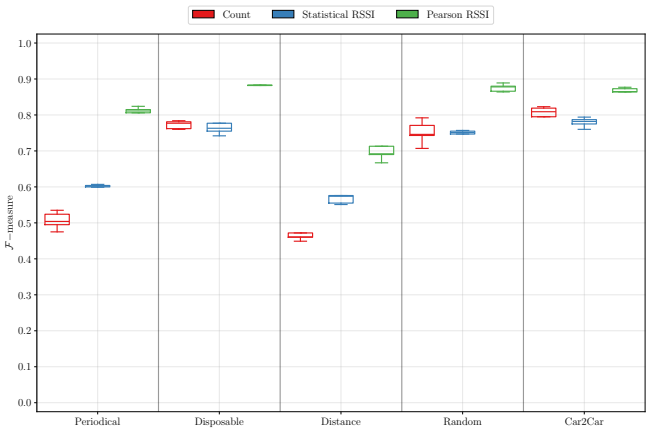

Fig. 3: Comparison of the $Count$, $Statistical\ RSSI$ and $Pearson\ RSSI$ metrics for tracking vehicles using a BSM sending frequency of 1 Hz.

The results presented in Figure 3 clearly highlight that the *Pearson RSSI* metric outperforms both *Count* and *Statistical RSSI* against all the pseudonym-changing schemes available in F^2MD. Overall, we highlight that the pseudonym-changing scheme with the lowest $\mathcal{F}_1$-measure value is the *Distance* scheme, where the pseudonym is changed based on the distance traveled by the vehicle.

C. Comparison with previous works

In this section we present a two-fold comparison with previous work. We use the pseudonym-changing schemes presented in [12] and the tracking methodology introduced in [13] (named *SLOWTrack*) to compare RADAR against pseudonym-changing schemes not available in F^2MD and against a different pseudonym-tracking methodology. For the sake of completeness, we also evaluate the tracking performance of *SLOWTrack* [13] against the hardest pseudonym-changing scheme for RADAR (*Distance*). We remark that there are no public implementations of either the pseudonym-changing schemes presented in [12] or the *SLOWTrack* [13] tracking methodology. Hence, the results presented in this section are obtained by re-implementing both the schemes and the tracking algorithm based on the description available in the original works. Hence the comparison presented in this section has the two-fold objective of (i) comparing RADAR with related work and (ii) serving as a benchmark for future advancements. As an additional contribution to the state-of-the-art, we publicly release all the implementations and simulation setups used in this work [1].

The results of this comparison are summarized in Figure 4, where the $\mathcal{F}_1$-measure achieved with RADAR (*Pearson RSSI* metric, green box-plot) is compared against *SLOWTrack* [13] (pink box-plot).

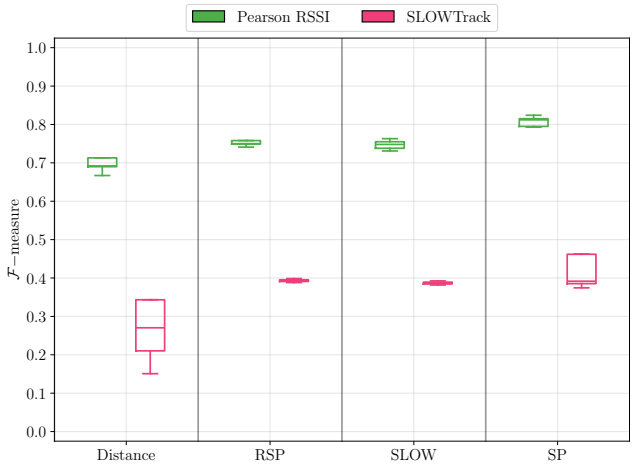

Fig. 4: Experimental comparison of the *Pearson RSSI* metric against the *SLOWTrack* methodology over different pseudonym-changing schemes.

From the analysis of the results presented in Figure 4 it is clear that RADAR outperforms *SLOWTrack* in all simulated scenarios, reaching peak performance that is twice that of achieved by the other solution. The main cause of the low tracking performance of *SLOWTrack* lies in the pseudonym-changing schemes used in our evaluation. In fact, all the pseudonym-changing schemes used in this comparison are based on a variable radio-silent period during which the pseudonym used by each vehicle is changed. However, in the original *SLOWTrack* [13] manuscript pseudonyms are tracked by "*joining the dots* between two heartbeat messages [...] or by constructing a trajectory through a consistent series of (position, velocity) pairs [...]". This implies that, by using a radio-silent period in pseudonym-changing schemes, the tracking performance of *SLOWTrack* is inversely proportional to the number of vehicles used in the simulation, while RADAR is mostly unaffected. Hence, this demonstrates that our tracking methodology based on multiple radio sources is more resilient to radio-silence periods, thus effectively tracking vehicles in VANET communication.

VI. Conclusions

In this work we presented RADAR, a tracking algorithm designed to exploit DSRC communication and Wi-Fi probe broadcast messages to bypass pseudonym-changing schemes and other privacy-preserving mechanisms in VANETs communication. The experimental evaluation of RADAR discusses three different metrics for tracking different pseudonyms belonging to the same vehicle, demonstrating that the metric based on the Pearson correlation between two series of RSSI signals (*Pearson RSSI*) outperforms the other two metrics in the worst-case scenario, where messages are sent with a frequency of 1 Hz, against 5 different pseudonym-changing

schemes. Experimental comparison against previous tracking algorithms and different pseudonym-changing schemes shows that RADAR is able to achieve higher tracking performance in all scenarios, and is more resilient to radio-silent periods and missing data than previous work. We remark that these results highlight the need for stronger, multi-layered privacy-preserving solutions that account all the communications emitted from the vehicles and their passengers to effectively preserve the privacy of road users in VANETs communication. As a final contribution, we also publicly release all the implementations and simulation setups used in this work [1] to overcome current limitations on reproducibility of previous work.

ACKNOWLEDGEMENTS

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.

This work has been supported by the Cyber Risks of Vehicle-to-Vehicle Communications (CRV2V) project (J33C22002810001) under the Cascade Open Calls of SERICS "CRV2V – Cyber Risks of Vehicle-to-Vehicle Communications" (PE00000014) founded by MUR National Recovery and Resilience Plan.

REFERENCES

[1] Gambigliani Zoccoli, Giovanni and Valgimigli, Filip and Stabili, Dario and Marchetti, Mirco. (Last visited Apr., 2025) RADAR: a Radio-based Analytics for Dynamic Association and Recognition of pseudonyms in VANETs - Implmentations. https://github.com/SECloudUNIMORE/ACS.

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

[4] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[5] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE communications surveys & tutorials*, vol. 17, no. 1, pp. 228–255, 2014.

[6] M. Gerlach and F. Guttler, "Privacy in vanets using changing pseudonyms-ideal and real," in *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring*. IEEE, 2007, pp. 2521–2525.

[7] European Telecommunications Standards Institute (ETSI), "Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management," ETSI, Tech. Rep. TR 103 415 V1.1.1, Apr. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf

[8] G. G. Zoccoli, D. Stabili, and M. Marchetti, "Are VANETs pseudonyms effective? An experimental evaluation of pseudonym tracking in adversarial scenario," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*. IEEE, 2023, pp. 1–6.

[9] L. Benarous, B. Kadri, and S. Boudjit, "Alloyed pseudonym change strategy for location privacy in vanets," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2020, pp. 1–6.

[10] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2018.

[11] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on Intersection Collision Avoidance systems," in *2013 IEEE Vehicular Networking Conference*, 2013, pp. 71–78.

[12] P. K. Singh, S. N. Gowtham, S. Nandi *et al.*, "CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs," *Vehicular Communications*, vol. 20, p. 100183, 2019.

[13] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *2009 IEEE vehicular networking conference (VNC)*. IEEE, 2009, pp. 1–8.

[14] I. Huso, S. Sciancalepore, G. Oligeri, G. Piro, and G. Boggia, "Frequency matters: On the impact of carrier frequency on privacy in radio fingerprinting," *IEEE Wireless Communications Letters*, 2025.

[15] M. Irfan, S. Sciancalepore, and G. Oligeri, "Preventing radio fingerprinting through friendly jamming," *arXiv preprint arXiv:2407.08311*, 2024.

[16] 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.

[17] M. Klapež, C. A. Grazia, and M. Casoni, "Experimental evaluation of ieee 802.11 p in high-speed trials for safety-related applications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11 538–11 553, 2021.

[18] [Online]. Available: http://dx.doi.org/10.4271/J2945/1_201603

[19] SAE International, "Dedicated short range communications (dsrc) message set dictionary," *SAE International*, 2016.

[20] IEEE, "Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages," Std. 1609.2-2022.

[21] European Telecommunications Standards Institute (ETSI), "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2," ETSI, Tech. Rep. TS 102 941 V2.2.1, 2022.

[22] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in vanets," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599–1609, 2013.

[23] 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.

[24] 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

[25] S. Wang, N. Yao, N. Gong, and Z. Gao, "A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs," *Peer-to-Peer Networking and applications*, vol. 11, pp. 548–560, 2018.

[26] "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)*, pp. 1–4379, 2021.

[27] *Core Specification*, Bluetooth Special Interest Group, 8 2024, v6.

[28] S. Gryś, "An experimental test bench for the tire pressure monitoring system–discussion of measurement and communication issues," *International Journal of Electronics and Telecommunications*, pp. 51–56, 2019.

[29] P. Sedgwick, "Pearson's correlation coefficient," *Bmj*, vol. 345, 2012.

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

[31] 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).

[32] 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.

[33] (Last visited Apr. 2025) MASA: Modena Automotive Smart Area. https://www.automotivesmartarea.it/?lang=en.

[34] 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.

[35] 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.