2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring) | 978-1-7281-8964-2/20/$31.00 ©2021 IEEE | DOI: 10.1109/VTC2021-Spring51267.2021.9449078

How well can your car be tracked: Analysis of the European C-ITS pseudonym scheme

Stephan Escher, Markus Sontowski, Knut Berling, Stefan Köpsell and Thorsten Strufe
TU Dresden, Germany
<firstname.lastname>@tu-dresden.de

***Abstract*—The change of pseudonym certificates for message authentication is the standard approach for privacy-friendly V2X communication. It's crucial to use an effective and robust pseudonym changing scheme as the location privacy of vehicles relies strongly on it. Therefore, in this work we analyzed a pseudonym change strategy that is recommended by the European C-ITS platform and has good chances to be included in a future European standard. By simulating a realistic urban traffic scenario within Luxembourg, applying and attacking the pseudonym change strategy, we could evaluate the effectiveness of the scheme. Overall, linking pseudonyms with simple traffic statistics in a realistic city traffic scenario is more challenging than related work suggests. However, the consideration of additional static information from the V2X communication, such as length and width of the vehicle, enormously improves the linking of pseudonyms, and thus enables tracking of vehicles and generation of motion profiles. The level of location privacy is thereby particularly influenced by the number of vehicles in the vicinity and especially their properties, as well as, of course, by the observation capabilities of the attacker. Our results suggest that the introduction of VANETs, even with the C-ITS pseudonym scheme, enables the tracking of vehicles, and thus will decrease location privacy in the future.**

***Index Terms*—V2X, VANET, ITS, location privacy, tracking, pseudonym change**

I. Introduction

Cooperative Intelligent Transportation Systems (C-ITS) enable wireless communication between vehicles (V2V) as well as surrounding transport infrastructure (V2I), summarized as vehicle to everything communication (V2X). This is achieved by vehicles using their on-board units (OBU) to regularly send data such as position, speed or direction by broadcasting to all receivers in the vicinity and to receive broadcast messages from other surrounding vehicles or the infrastructure via road side units (RSUs). This enables so-called vehicular ad hoc networks (VANETs), whose participants are always informed about vehicles in the vicinity. Shared information can be used, e.g. to avoid collisions by coordinated vehicle movements, to warn about accidents and traffic jams, or for intelligent traffic light control, thus ensuring safer and more efficient road traffic overall.

In order to ensure that the information is not faulty or manipulated, common systems rely on the authentication of sent messages by means of digital signatures and certificates. Each recipient can determine the authorization of the sender using these signatures and verify the integrity of the message.

However, this approach poses major problems for the protection of the vehicle's private data and thus also of the driver. Every vehicle exposes its identity and further information such as its exact position to its environment. Hence, the introduction of V2X communication can facilitate the tracking of vehicles and thus the creation of motion profiles.

One common solution is to pseudonymize the communication. Instead of using one signature, that unambiguously identifies a specific vehicle, a vehicle would use a number of different signatures which are changed while driving according to a specific change strategy. Overall it is important to use an effective and robust pseudonym changing scheme as the effectiveness of the protection of vehicles data privacy relies strongly on it. A major issue with pseudonym changing schemes is that pseudonyms might be linked and therefore, a trajectory can be reconstructed or vehicles even can be deanonymized.

Thus in this work we analyse a pseudonym change strategy, which is recommended in the security guidelines of the European C-ITS platform and has good chances to be included in a future European standard [1]. By simulating a realistic traffic scenario and attacking the applied pseudonym scheme, we try to determine to what extent it effectively prevents vehicle tracking.

II. Related Work

The topic of pseudonymization of vehicles in VANETs is being addressed in a large amount of work. A detailed overview is given by Petit et al. [2]. They give an insight into the functioning of pseudonyms and present an abstract life cycle of pseudonyms as well as various implementations in concrete pseudonym schemes. Boualouache et al. [3] give a comprehensive overview of pseudonym change strategies and classify them according to various characteristics. Wiedersheim et al. [4] showed in their work that simple pseudonym changes do not provide satisfactory pseudonymization, since it is easy for an attacker to link pseudonyms which are changed in the observation areas.

Troncoso et al. [5] carried out a successful attack on the asymmetric pseudonym change strategy in the US model IntelliDrive using a simple urban traffic simulation. The scenario used is rather unrealistic and the attack carried out cannot be transferred to the European model.

This work has been supported in part by the Federal Ministry of Education and Research of the Federal Republic of Germany (BMBF) in the framework of the project 5GNetMobil with funding number 16KIS0689. The authors alone are responsible for the content of the paper.

978-1-7281-8964-2/21/$31.00 ©2021 IEEE

Buttyán et al. [6] introduced the concept of mix zones for vehicular pseudonym schemes, which is helpful for the analysis of the effectiveness of pseudonym changing strategies. They simulated a realistic traffic scenario based on real streets within Budapest. Nevertheless, the street map of Budapest's city centre is highly simplified and limited to a few major roads. In addition, the simulation artificially determines how many vehicles appear in traffic.

Förster et al. [7] presented a framework for the evaluation of pseudonym change strategies, with the help of which different steps in an evaluation can be conceptually well analysed. They based their work on the findings of Buttyán et al. [6]. Additional they presented a new type of attack strategy and applied it with good success to the Budapest scenario. They analysed two different pseudonym change strategies.

To the best of our knowledge, there is no study which uses realistic traffic scenarios to address the issue of traffic complexity.

III. The European Pseudonym Scheme

For the European context, security and privacy of V2X communication are primarily defined by the EU's C-ITS Platform, whose policies build upon specifications of the European Telecommunications Standards Institute (ETSI). The C-ITS platform's security policy [1] and certificate policy [8] are envisaged to govern security, privacy and trust aspects of ITS deployment within the EU. The certificate policy defines the European C-ITS trust model and builds upon the PKI architecture presented in [9]. The security policy [1] proposes legal entities and bodies to take over the roles defined in the certificate policy, defines security levels for several ITS message types and prescribes mandatory minimum controls for V2X communication. Further, the security policy defines a strategy for regular change of pseudonyms, based on a proposal by the Car-2-Car Communication Consortium (C2C-CC) [10]. The current version of the C-ITS security policy recommends the following pseudonym change strategy.

A. Pseudonym Change Strategy

The European C-ITS pseudonym change strategy considers a combination of changes according to fixed parameters and added random values. As a compromise between privacy and technical or economic feasibility, this strategy defines the objective, that at least 95% of all journeys can be divided into at least three segments. The basis for this numbers is the 'exemplary estimate' that 95% of all trips are longer than 10min or longer than 3km [10].

According to this strategy, the first pseudonym change occurs at the start of a new journey. The start of a new journey is considered when the vehicle's ignition was switched off for at least 10 minutes, the ignition is then switched on again and the vehicle is moving. The purpose of these conditions is to avoid that frequent shorter stops e.g. at traffic lights are counted and lead to a pseudonym change. The second pseudonym change takes place randomly within a distance of 800–1500m from the starting point of the journey. The third pseudonym change takes place minimal 800m after the last change and an additional driving time of 2–6min. The fourth pseudonym change takes place randomly between the next 10km–20km. Every further pseudonym change takes place randomly between every 25km–35km.

The minimum distance of 800m between two changes is intended to prevent the attacker from being able to observe several pseudonym changes from the same observation point. According to the C2C-CC, the average radio range in rural areas, with a clear view between transmitter and receiver, is about 300–500m and in urban areas it is sometimes less than 100m, due to the density of buildings, which is a radio obstacle [11]. Thus, the idea behind the minimum distance of 800m should work well at least in the area of a city.

B. V2X Message Content

As the C-ITS messages are not encrypted, its also important to consider the content, as it can potentially be used to track vehicles. According to ETSI, there are different types of messages for V2X communication, e.g. Cooperative Awareness Messages (CAMs) or Decentralized Environmental Notification Messages (DENMs) [12], [13]. Here we focus on CAM messages, which are the basis of V2X communication. CAMs are broadcasted periodically (e.g. 10Hz). They are unencrypted but signed with a certificate. The message contains mandatory and optional vehicle information [13]. For location privacy, certain information can be considered critical, e.g. vehicle position, direction, speed, or size. Besides position and time of a message, in this work we will also focus on vehicle width and length, since these parameters do not change over time and are therefore well suited for linking pseudonyms.

IV. Experimental Setup

Our analysis of the European C-ITS pseudoym scheme is based on the slightly customized framework described by Förster et al. [7], which allows the evaluation of different pseudonym change strategies and attackers. Overall the framework consists of five phases. These are *(i)* modeling vehicle mobility traces, *(ii)* applying the pseudonym change strategy onto mobility traces, *(iii)* observing parts of the pseudonymized traces, *(iv)* learning of traffic statistics and attacking the observed pseudonymized traces and finally *(v)* evaluate the success rate of the attacker. In the following the different steps are described in detail.

A. Traffic Simulation

In the first phase, mobility traces were generated using the SUMO traffic simulator [14]. For the traffic scenario we used the Luxembourg SUMO Traffic (LuST) [15], a realistic urban traffic scenario. It includes a very detailed road network of the medium-sized city of Luxembourg with a total of 931km of roads on a total area of 156km^2. The road network also includes traffic lights at crossroads, inductive loops, and polygons of buildings and car parks. In addition, the LuST-scenario provides traffic data generated for 24 hours. The generation of these data included extensive real information on

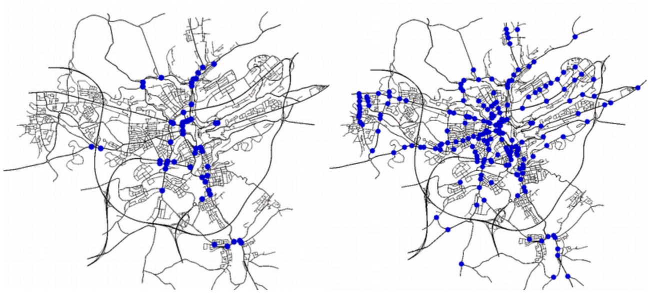

Fig. 1. Attacker with 50 (left) and 200 (right) observed junctions in the Luxembourg scenario.

the size and age structure of the population, schools, jobs and housing estates and known traffic characteristics of the city. The vehicle routes have been optimized so that the vehicles adapt their route to the traffic situation instead of choosing the shortest path. The LuST-scenario thus represents one of the best elaborated and most realistic scenarios available for SUMO. In this work, we modified the LuST scenario slightly. As the main goal is to analyse personal vehicles, we reduced the data set by excluding bus traffic. Additionally, we removed transit traffic as well as the traffic of all vehicles whose journey begins or ends outside the city. Both adjustments only slightly reduced the total traffic. We used the Traffic Control Interface API (TraCI API) from SUMO to execute the simulation and to extract the traces of each vehicle in a one second granularity (similar to CAM broadcast). Each trace contains the following information: Vehicle ID (VID), time (in sec), position (in SUMO coordinates) and traveled distance. The result is a set of all mobility traces T.

B. Adding Metadata

Since CAM messages also contain the vehicle length and width, we added both properties to the mobility traces in our simulation. To get a realistic assignment of vehicle sizes we used a snapshot of all registered vehicles running in Luxembourg from November 2019 [16]. Since the attacking scenario is designed to trace individual traffic, we focused only on registered vehicles in the main category M1 (motor vehicles designed and constructed primarily for the carriage of persons with max. nine seats [17]). This results in 322,359 vehicle entries with their type, brand and model. Because the official database did not contain any vehicle sizes we matched the given vehicle specifications with a database on vehicle properties[1] to get the size (in a granularity of decimetres) for each model. Finally, we randomly assigned a model with corresponding length and width to each simulated vehicle, according to the distribution of [16].

C. Applying the Pseudonym Change Strategy

In the next step the mobility traces T are pseudonymized according to the C-ITS pseudonym change strategy (see III-A). The result of this phase is a set of pseudonymized traces P={pseudonym, time, position, length, width}.

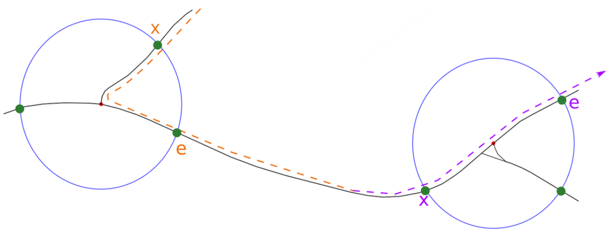

Fig. 2. Observation zones (blue) with 100m radius and fine granular observation points (road entries) in green. Mix zone traversal with pseudonym change (dashed lines) with exit and enter events.

D. Modelling the Attacker

We consider an attacker who has control of multiple observation points in the city, each point with a restricted observation radius of 100m, due to the limited range of the used V2X wireless technology (IEEE 802.11p or 5G sidelink). Observation points are stationed at traffic lights on junctions and therefore being able to observe all the traffic in and out of the junction in the observation radius. Similar attackers are also described by [7] and [6]. Further, we consider an observing attacker, who only listens but does not send messages nor tries to manipulate the communication.

The goal of the attacker is to track vehicles that change their pseudonym between two observation zones, i.e. the goal is to link different pseudonyms of the same vehicle. Everything outside the observation zone is called *mix zone*. We considered three attackers of different strength with observation points at 50, 100 and 200 intersections (see Fig. 1).

E. Observing Vehicles

To simulate the modelled attacker the set of pseudonymized traces P is reduced by the traces whose position is not within the observation range, which was done with the context subscription function of the TraCI API. The result is a set of observed pseudonymized traces O. From O it can be determined whether pseudonym changes have occurred within the observation zones. These observed changes can easily be linked by the attacker [4]. After linking all pseudonym changes which have taken place in the observation area, the observed pseudonymized traces are reduced to *exit* and *enter* events, resulting in event traces E. An exit event describes an observed pseudonymized trace where the vehicle leaves the mix zone and enters the observation zone. The enter event describes the trace where the vehicle leaves the observation zone and enters the mix zone (see also Fig. 2).

F. Learning Traffic Statistics

During the fourth phase, the attacker executes his attack on the set of observed traces. His aim is to track vehicles driving through the mix zone, i.e. to find out which enter events belong to which exit events, even if the pseudonym has changed. To make this possible, the attacker first has to

[1] https://www.cars-data.com

Algorithm 1 weight (e,x)

```
if $e.time >= x.time$ then
    return $0$
else if $e.length \neq x.length$ or $e.width \neq x.width$ then
    return $0$
else if $no\ trip\ from\ e.position\ to\ x.position\ in\ statistics$ then
    return $0$
else if $travel\_time > max\_time$ or
  $travel\_time < min\_time$ then
    return $0$
else if $(travel\_time = avg\_time)$ then
    return $nr\_vehicles$
end if
return $nr\_vehicles\ /\ abs(travel\_time - avg\_time)$
```

generate knowledge about the traffic flow in the city. Therefore he uses the data of observed vehicles that have not changed their pseudonym between entering and leaving the mix zone to build up statistics. In this way, for each pair of observation zones, the attacker can record the number of vehicles that travel back and forth between the points, as well as the average time it took them.

To improve the original approach [7], we added fine granular observation points (road entries) to the observation zones and map each event to the nearest fine granular point (see Fig. 2). Thus, the statistics are not generated for pairs of observation zones but for fine granular pairs of road entries of observation zones. The learned statistics about how many vehicles drove through such a pair of observation points and how long it took them on average are finally used to attack the pseudonym changes between these points, i.e. to track vehicles traveling through the mix zones.

G. Attacking the Pseudonymization Scheme

The attack consists of the attacker using all events that have not yet been matched with any other event during learning to construct a weighted bipartite graph. Each node in this graph represents a particular event. Each edge connects an enter event with an exit event. The weight of these edges represents the probability that the corresponding events belong to the same vehicle. For the calculation of the weight the statistical data obtained during learning is used. The weight of the edge (see Algorithm 1) between an enter event *e*, observed at the fine granular observation point *e.position*, and an exit event *x*, observed at *x.position*, increases the more vehicles (*nr_vehicles*) previously traveled between *e.position* and *x.position*. It decreases the more the time interval between the two events (*travel_time*) deviates from the average time (*avg_time*) measured between *e.position* and *x.position*. Beforehand, to improve the attack by [7], we added a validity check using the minimal and maximal learned time and added a safety margin to make sure the matched results could be realistically possible and to reduce the size of the graph of matched sets. Additionally, we excluded all exit-enter event pairs which are not of the same vehicle length and width. After the graph has been constructed, that matching is calculated, for which the graph reaches a maximum cardinality and a maximum weight. The attack is not only applied once to all events in the database, but the registered events are processed at intervals of a certain length *t*. The length of the time intervals between the individual executions of the attack determines the size of the resulting graph and thus the size of the graph matching problem. Here, an attack interval of 300s was selected. Within the interval all enter events between t_0 and t_{300} and all exit events between t_0 and t_{600} are collected. Then the weight between all pairs of exit and enter events is calculated. Unmatched exit events between t_{300} and t_{600} will be used again in the following attack interval. The output of the attack is a set of matches M, which are the decisions of the attacker of which pseudonyms belong to the same vehicle.

TABLE I
NUMBER OF PSEUDONYM CHANGES PER VEHICLE.

nr. of changes	1	2	3	4
nr. of vehicles	2,758	38,900	168,444	4,213
percent	1.3%	18.2%	78.6%	2.0%

H. Evaluating Attack Success

In the last phase, the success of the attacker is evaluated by comparing the traces reconstructed by him, represented by the set of matches M, with the original mobility traces T from the first phase.

V. Evaluation

A. Mobility Simulation

In total, the simulated traffic comprised 214,315 vehicles with overall 209,654,111 mobility traces T. The average travel time is 16.33min and the average travel distance is 8.62km. In total, the vehicles performed 602,742 pseudonym changes. The number of pseudonym changes made during the journey per vehicle can be seen in Table I. 1.3% of the vehicles performed only one change during their journey (at the start); 18.2% completed two and 78.6% three changes. Thus, in this realistic traffic scenario, the specified goal of the pseudonym change to divide the journey of at least 95% of the vehicles into 3 segments, is not achieved. However, this assumption can also be questioned in general when considering various traffic studies, e.g. in Germany [18], [19].

B. Width and Length of Vehicles

Considering the distribution of registered vehicles and their properties in Luxembourg, we can identify an issue of pseudonymization in general. A number of 99 (0.03%) vehicles had such a unique combination of length and width that they were only once registered in Luxembourg and thus could always be tracked. Additionally 18,903 (5.86%) vehicles have a size that they share with less than 100 other vehicles (72 sizes for which only 2 vehicles exist). These vehicles, although not unique, can simply be deanonymized, as it is very unlikely that a vehicle of the same size will be at the same time in the vicinity. On the other hand, there are also 8,703 (2.67%) vehicles, which are of the same size. Hence, drivers driving vehicles of this class are more likely not to be tracked, due to a higher probability of other vehicles of the

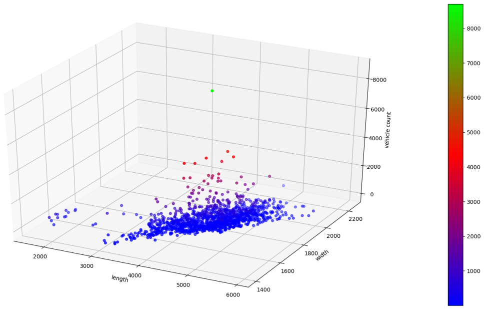

Fig. 3. Distribution of registered vehicles in Luxembourg regarding size properties (length and width).

TABLE II

Observation Zones	200	100	50
Nr. of vehicles	205,497	195,813	169,028
% of all vehicles	95.89%	91.36%	78.87%
Observed changes	86,605	64,736	41,778
% of all changes	14.37%	10.74%	6.93%
Mix Traversals	152,037	115,965	67,693

same size in the area. The whole distribution of size properties can be seen in Fig. 3.

C. The Attacker View — Observing Vehicles

The attacker's observations and attack capabilities naturally vary with the number of observation points. Table II gives a general overview about observation possibilities of the attacker. With 200 observation points within the city, the attacker can see overall 95.89% of all vehicles driving through Luxembourg. Furthermore, he can directly observe 86,605 pseudonym changes, because they were performed within an observation zone. Overall, with 200 observed junctions, there are 152,037 mix zone traversals, where a vehicle leaves an observation zone and enters another one with a changed pseudonym (independent on how often it changes between the two points).

D. Linking Pseudonyms of Mix Zone Traversals

Next to directly observed pseudonym changes, the attacker tries to link mix zone traversals, i.e. link exit and enter events to a specific vehicle even if it changed the pseudonym. With the slightly modified original attack (only position and time), the attack success, compared to [7], is rather poor (see Table III-1). A possible reason could be the realistic traffic scenario: The road network is extensive, so that vehicles can travel from one observation point to the next in several different ways; traffic light waiting times and possible traffic jams cause delays in the traffic flow. These reasons mean that the average travel times measured from point to point are less meaningful. Additional false positive rates are not mentioned by [7].

However, adding the static vehicle characteristics of length and width to the attack, the success rate increases enormously (see Table III-2). With 200 observed intersections within Luxembourg, the attacker was able to correctly link an enter with an exit event, and thus the pseudonyms of the corresponding vehicle, with $> 70\%$ precision. It can also be seen that the number of observation points has a high influence on the success rate of the attacker. The smaller the observation possibilities the worse the precision of linking. One reason for this is an increased number of events which have no counterpart in the observation area, but which could erroneously be matched with another event.

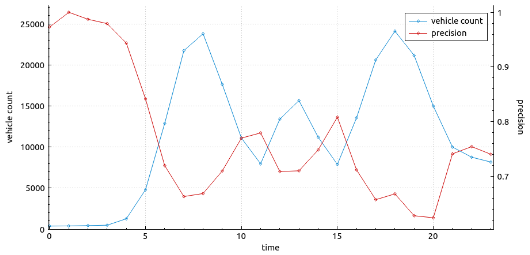

Fig. 4. Correlation between traffic volume and precision of the attack.

TABLE III

Observation Zones	200	100	50
Mix Traversals	152,037	115,965	67,693
1) Linking with Position and Time			
Precision	11.87%	7.50%	5.25%
Recall	20.44%	15.46%	13.31%
F1-Score	15.02%	10.10%	7.53%
2) Linking with Position, Time and Size			
Precision	71.12%	59.46%	50.87%
Recall	76.14%	71.62%	73.91%
F1-Score	73.55%	64.98%	60.26%

The influence of traffic volume on the success of the attacker can be seen in Fig. 4. An increased traffic flow decreases the precision of the attacker. This was expected, as more vehicles with the same size characteristics appear side by side in the observation zones and therefore more event combinations occur.

E. Linking the Entire Journey of Vehicles

Table IV shows the distribution of mix zone traversals per vehicle as well as the attacker's success in linking the entire journey of them. Entire journey means the tracking of a vehicle from the moment the attacker observed it for the first time until the last time. The number of mix traversals describes how often the vehicle appears with different pseudonyms, i.e. mix zone traversals the attacker has to link correctly to follow the entire route of the vehicle.

Vehicles with zero mix zone traversals can be directly followed over the entire route, cause they either have been observed only briefly or they performed their pseudonym changes directly within observation zones. Vehicles with three mix zone traversals had 4 pseudonym changes (first at start, see Tab. I), which have all taken place unobserved by the attacker (within the mix zone). After all, about 60% of these cases could be linked correctly. Trips that were divided into

TABLE IV
MIX TRAVERSAL POSSIBLY LINKED BY THE ATTACKER

Observation Zones	200	100	50
Observed Vehicles	205,497	195,814	169,029
Linked Journeys	82.99%	83.64%	89.75%
0 Mix Traversals	83,822	97,012	107,616
Linked	100%	100%	100%
1 Mix Traversals	91,624	81,793	55,144
Linked	73.88%	69.03%	73.07%
2 Mix Traversals	29,740	16,855	6,258
Linked	63.28%	60.75%	60.64%
3 Mix Traversals	311	154	11
Linked	63.02%	51.30%	72.72%

3 segments (2 mix zone traversals), which is the goal of the C-ITS peudonym change, could be linked with a success rate of $> 60\%$.

Overall $> 80\%$ of observed vehicles could be linked over the entire route, regardless of the number of observation stations. Even though the success rate of the attacker decreases with an increasing number of mix zone traversals, tracking cannot be prevented effectively. The creation of comprehensive motion profiles is especially feasible for stronger attackers (e.g. RSUs such as traffic light systems), as success depends on the distribution and count of the observation points. However, targeted attacks are also conceivable, for example on special points of interest such as workplaces (e.g. police station) in order to find out who works there, where a person lives or when she comes to work. Thus, observation stations can be set up in a targeted and gradual manner.

VI. Conclusion

In this work we used the slightly improved framework from Förster et al. [7] to analyse the effectiveness of a pseudonym change strategy, recommended by the European C-ITS platform. For this purpose, we simulated a realistic urban traffic scenario within Luxembourg and added realistic vehicle characteristics of width and length, which are transmitted via V2X communication. Further, we modelled attackers of different strength (number of observation points), which try to link pseudonym changes with the help of learned traffic statistics and vehicle properties.

Overall, linking pseudonyms with simple traffic statistics within a realistic city scenario is more challenging than related work suggests. However, the consideration of additional information from the V2X communication, such as length and width of the vehicle, enormously improves the linking of pseudonyms, and thus enables tracking of vehicles and generation of motion profiles. Around 80% of the vehicles observed could be tracked from the first to the last observation point, regardless of the strength of the attacker. However, the stronger the attacker, the more vehicles and longer distances can, of course, be observed. Furthermore, the precision of the attack increases with the number of observation points. Besides the observation possibilities, the success of the attacker is also particularly influenced by the number of vehicles in the vicinity and especially their properties. For example, the length and width of a vehicle can be unique in its vicinity, so that the attacker can clearly track this vehicle, regardless of the pseudonym scheme used. In addition to length and width, further information such as Wi-Fi or Bluetooth identifiers, could potentially be used to bridge the pseudonym change. Furthermore, improved attacks, which are not only based on simple traffic statistics, e.g. with more information about the road network, and with improved learning algorithms could increase the success of linking pseudonyms.

Overall, our results suggest that the introduction of VANETs, even with the C-ITS pseudonym scheme, enables the tracking of vehicles, and thus decreases location privacy in the future.

References

[1] EuropeanCommision, "Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) – Release 1," 2017.

[2] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE communications surveys & tutorials*, 2014.

[3] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, 2017.

[4] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *WONS*, 2010.

[5] C. Troncoso, E. Costa-Montenegro, C. Diaz, and S. Schiffner, "On the difficulty of achieving anonymity for vehicle-2-x communication," *Computer Networks*, 2011.

[6] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *ESAS*, 2007.

[7] D. Förster, F. Kargl, and H. Löhr, "A framework for evaluating pseudonym strategies in vehicular ad-hoc networks," in *WiSec*, 2015.

[8] EuropeanCommision, "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) – Release 1," 2017.

[9] ETSI, TS 102 940 (v1.3.1) - Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, 2018.

[10] ETSI, TR 103 415 (v1.1.1) - Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management, 2018.

[11] C2C-CC, "FAQ regarding Data Protection in C-ITS," 2018.

[12] ETSI EN 302 637-3: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, Version 1.2.1, 2014.

[13] ETSI EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, Version 1.3.1, 2014.

[14] 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 *ITSC*, 2018.

[15] L. Codeca, R. Frank, and T. Engel, "Luxembourg sumo traffic (lust) scenario: 24 hours of mobility for vehicular networking research," in *VNC*, 2015.

[16] "Parc automobile du luxembourg," https://data.public.lu/fr/datasets/parc-automobile-du-luxembourg/, Le Gouvernement Luxembourg, accessed: 2019-12.

[17] EuropeanUnion, "Regulation (eu) 2018/858 of the european parliament and of the council," 2018.

[18] M. Wermuth, C. Neef, R. Wirth, I. Hanitz, H. Löhner, H. Hautzinger, W. Stock, M. Pfeifer, M. Fuchs, B. Lenz *et al.*, "Kraftfahrzeugverkehr in Deutschland 2010," *WVI, IVT DLR and KBA*, 2010.

[19] DLR, infas. "Mobilität in Deutschland – Tabellarische Grundauswertung – Verkehrsaufkommen – Struktur – Trends", 2018.